VOL. 17 NO. 2 JUNI 2016

ISSN : 1411-3201

Jurnal Ilmiah DASI

DATA MANAJEMEN DAN TEKNOLOGI INFORMASI

STMIK AMIKOM
YOGYAKARTA

VOL. 17 NO. 2 JUNI 2016
JURNAL ILMIAH
Data Manajemen Dan Teknologi Informasi

Terbit empat kali setahun pada bulan Maret, Juni, September dan Desember berisi artikel hasil penelitian dan kajian analitis kritis di dalam bidang manajemen informatika dan teknologi informatika. ISSN 1411-3201, diterbitkan pertama kali pada tahun 2000.

PENANGGUNG JAWAB :
Ketua STMIK AMIKOM Yogyakarta, Prof. Dr. M. Suyanto, M.M.

ALAMAT PENYUNTING & TATA USAHA
STMIK AMIKOM Yogyakarta, Jl. Ring Road Utara Condong Catur Yogyakarta, Telp. (0274) 884201 Fax. (0274) 884208, Email : jurnal@amikom.ac.id

BERLANGGANAN
Langganan dapat dilakukan dengan pemesanan untuk minimal 4 edisi (1 tahun) pulau jawa Rp. 50.000 x 4 = Rp. 200.000,00 untuk luar jawa ditambah ongkos kirim.

DAFTAR ISI

HALAMAN JUDUL…… i

KATA PENGANTAR ii

DAFTAR ISI..... iii

Implementasi Algoritma K-Nearest Neighbor dalam Memprediksi Potensi Calon Kreditur Di KSP Galih Manunggal ……..……..…….……1-6
Agung Nugroho
(Sistem Informasi STMIK AMIKOM Yogyakarta)

Implementasi VPN Server dalam Sistem Informasi Apotek (Studi Kasus Integrasi Sistem Informasi Apotek Santi Pontianak)…….…….…… ……7-12
Anang Masykuri[1)], Ema Utami [2)], Sudarmawan[3)]
([1)]SMA Negeri 4 Pontianak, [2,3)]Teknik Informatika STMIK AMIKOM Yogyakarta)

Perancangan Sistem Informasi Akademik Berbasis Web di Akademi Kesehatan Sapta Bakti Bengkulu ……..…….……13-20
Andika Wendi Febrian[1)], Kusrini[2)], M. Rudyanto Arief [3)]
([1)]Teknik Informatika STMIK AMIKOM Yogyakarta, [2,3)]Magister Teknik Informatika STMIK AMIKOM Yogyakarta)

Image Matting untuk Ekstraksi Objek Rambut pada Citra Digital…….....21-30
Anyan[1)], Ema Utami[2)], Amir Fatah Sofyan[3)]
([1)]STKIP Persada Khatlistiwa Sintang, [2)]Magister Teknik Informatika STMIK AMIKOM Yogyakarta, [3)]Teknik Informatika STMIK AMIKOM Yogyakarta)

Perancangan Sistem Informasi Pendaftaran Mahasiswa Aktif Kembali di STMIK AMIKOM Yogyakarta…….……..……...……..31-37
Eli Pujastuti
(Teknik Informatika STMIK AMIKOM Yogyakarta)

Sistem Pendukung Keputusan Penilaian Kinerja Dosen Sebagai Pemandu Usulan Kenaikan Jabatan Akademik..…….. ……..…..…….38-45
Indyah Hartami Santi[1)] , Ema Utami[2)], Armadyah Amborowati[3)]
([1)]Teknik Informatika Universitas Islam Balitar Blitar, [2)]Magister Teknik Informatika STMIK AMIKOM Yogyakarta, [3)]Teknik Informatika STMIK AMIKOM Yogyakarta)

Perencanaan Strategis Sistem Informasi untuk Pengelolaan Kepemimpinan di Sekolah Muhammadiyah Kota Yogyakarta……...……..…..…….46-52
Jefree Fahana[1)], Ema Utami[2)], Armadyah Amborowati[3)]
([1)]Majelis Dikdasmen Pimpinan Wilayah Muhammadiyah D.I.Yogyakarta, [2)]Magister Teknik Informatika STMIK AMIKOM Yogyakarta, [3)]Teknik Informatika STMIK AMIKOM Yogyakarta)

Analisis dan Perancangan Sistem E-Filing Standard Operating Procedure Menggunakan Five Core Workflow Rational Unified Proses……...……53-61
Lukman
(Teknik Informatika STMIK AMIKOM Yogyakarta)

Sistem Penunjang Keputusan untuk Seleksi Calon Guru Menggunakan Analytical Hierarchy Process (AHP)… ……..…….…….....62-66
Mulia Sulistiyono
(Teknik Informatika STMIK AMIKOM Yogyakarta)

Sistem Pakar E-Tourism pada Dinas Pariwisata D.I.Y Menggunakan Metode Forward Chaining ……...……...……..…….67-75
Rizki Wahyudi[1)], Ema Utami[2)], M. Rudyanto Arief[3)]
([1)]AMIK-AKTAN "Boekittinggi", [2,3)]Magister Teknik Informatika STMIK AMIKOM Yogyakarta)

Indeks Penilaian Tingkat Kematangan (Maturity) IT Governance pada Manajemen Keamanan Layanan Teknologi Informasi…….…….76-82
Robert Marco
(Teknik Informatika STMIK AMIKOM Yogyakarta)

Studi Deskriptif Pola Pemanfaatan Free Wi-Fi Berdasarkan Konten yang Diakses pada Mahasiswa STMIK AMIKOM Yogyakarta……..…83-87
Sri Mulyatun[1)], Sri Ngudi Wahyuni[2)]
([1)]Manajemen Informatika STMIK AMIKOM Yogyakarta, [2)]Teknik Informatika STMIK AMIKOM Yogyakarta)

INDEKS PENILAIAN TINGKAT KEMATANGAN (*MATURITY*) *IT GOVERNANCE* PADA MANAJEMEN KEAMANAN LAYANAN TEKNOLOGI INFORMASI

Robert Marco

Teknik Informatika STMIK AMIKOM Yogyakarta
email : robertmarco@amikom.ac.id[1)]

Abstraksi

Perguruan Tinggi selain memiliki bagian Satuan Penjamin Mutu, Perguruan Tinggi juga memiliki bagian Satuan Pengendalian Internal atau Auditor Internal, khususnya dalam manajemen keamanan informasi terhadap penyelenggara layanan publik, terkait dengan manajemen keamanan layanan dan melakukan pengontrolan pelaksanaan manajemen layanan. Metode penelitian yang digunakan adalah metode deskriptif dengan pendekatan penelitian kualitatif dan kuantitatif. Sasaran evaluasi penelitian adalah tata kelola TI dalam keamanan layanan informasi. Menilai kelengkapan pengamanan 5 area Penilaian dalam Indeks ISMS dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2009, yang disusun kembali menjadi 5 (lima) area. Dalam penelitian ini, Jurusan STMIK AMIKOM memiliki kekurangan pada keamanan informasi disebabkan karena belum adanya kontrol, aturan, kebijakan, standar untuk perlindungan keamanan informasi. Belum adanya pencatatan maupun dokumentasi secara berkala mengenai insiden kelemahan keamanan informasi yang disebabkan karena tidak terdapat kebijakan, prosedur maupun aturan untuk menanggulangi insiden kelemahan terhadap keamanan informasi.

Kata Kunci :
ISO 27001, Keamanan Teknologi Informasi, Manajemen Layanan, Maturity, ISMS

Abstract

Universities in addition to having part of the Quality Assurance Unit, Higher Education also has a section Internal Control Unit or Internal Auditor, particularly in the management of information security to the public service providers, related to security management services and controlling the implementation of the service management. The method used is descriptive method with qualitative and quantitative research approaches. Target evaluation is IT governance research in information security services. 5 assess the completeness of security in the Index area ISMS assessment done by the overall scope of the security requirements specified in the standard ISO / IEC 27001: 2009, which was reorganized into five (5) areas. In this study, the Department STMIK AMIKOM have a deficiency in information security due to the absence of control, rules, policies, standards for information security protection. The absence of regular recording and documentation regarding incidents of information security weaknesses that are caused because there are no policies, procedures and rules to overcome weaknesses to information security incidents.

Keywords:
ISO 27001, Information Technology Security, Service Management, Maturity, ISMS.

Pendahuluan

Perguruan tinggi khususnya perguruan tinggi swasta pada perkembangannya mempunyai kecenderungan untuk mengadopsi Teknologi Informasi untuk menjalankan bisnisnya. Pengadopsian tersebut mengakibatkan perubahan peran, prosedur dan model audit yang perlu dijalankan pada linkungan perusahan yang mengadopsi TI pada proses bisnisnya, maka perlu adanya tata kelola teknologi informasi yang baik. Dengan adanya tata kelola TI, semua faktor dan dimensi yang berhubungan dengan penggunaan teknologi informasi menjadi bersinergi dan bisa memberikan nilai tambah yang diharapkan bagi perusahaan atau institusi.

Salah satu faktor yang dapat mempengaruhi keberhasilan integrasi institusi adalah dukungan dan manajemen sistem dan teknologi informasi yang dibutuhkan dalam kegiatan operasional kampus. Dalam kegiatan operasional tersebut, menjadi sangat tergantung pada keterdiaan dukungan teknologi informasi yang dibutuhkan secara kountinous dan aman. Penggunaan standar pelayanan dan keamanan dalam memandu proses bisnis menjadi salah satu solusinya akan tetapi organisasi memiliki kesulitan tersendiri untuk memahami sejauh mana standar tersebut telah terimplementasikan terlebih ketika organisasi mengimplemetasikan lebih dari satu buah standar.

STMIK AMIKOM yogyakarta, yang merupakan salah satu perguruan tinggi terbesar di yogyakarta yang bergerak dalam bidang IT (*Information Technology*). Dimana lembaga ini telah menerapkan teknologi informasi dalam proses manajemen untuk proses operasional lembaga. Untuk mengetahui tingkat kematangan (*maturity*) manajemen keamanan layanan di organisasinya, apakah penerapan selama

ini telah sesuai atau memenuhi standar terhadap penyelenggara layanan publik, terkait dengan manajemen keamanan layanan dan melakukan pengontrolan pelaksanaan manajemen layanan. Maka perlu adanya audit tata kelola teknologi informasi, sebagai faktor penentu tata kelola teknologi informasi, seperti strategi bisnis, tata kelola organisasi, ukuran organisasi, intensitas informasi, kestabilan lingkungan, dan kompetensi bisnis [1].

Tinjauan Pustaka

Penelitian Kusumah, P.; Sutikno, S.; Rosmansyah, Y. (2014), menyatakan bahwa keamanan informasi umumnya diselesaikan secara parsial dan terbatas. Hal ini juga terjadi untuk PPATK yang berlaku hanya wilayah pengelolaan keamanan informasi dengan mengadopsi ISO / IEC 27001: 2009 dan ISO / IEC 27002: 2005. Penelitian ini bertujuan untuk mengembangkan model penilaian proses yang mendukung penerapan tata keamanan informasi pada organisasi. Metode yang digunakan dalam penelitian ini adalah kualitatif Metode. Berdasarkan validasi oleh penilaian ahli, informasi Model tata kelola keamanan telah disusun sesuai dengan persyaratan keamanan informasi, khususnya di PPATK.

Budi Yuwono dan Annas Vijaya (2011), penelitian ini, ditujukan untuk menyelidiki setiap korelasi antara tata kelola TI perusahaan tingkat kematangan dan kinerja bisnis. tingkat kematangan tata kelola diukur menggunakan model kematangan disediakan oleh *Control Objective* untuk Informasi dan Teknologi Terkait (COBIT) versi 4.1. Penelitian dilakukan untuk mengeksplorasi efek waktu keterlambatan mengukur dampak dari tata kelola TI, dalam kesiapan untuk mengadopsi mekanisme tata kelola TI, tingkat organisasi ketergantungan pada TI, dan tingkat kompetensi anggota staf IT.

Humam Al Agha (2013), penelitian ini menemukan bukti empiris yang kuat tentang kematangan lima domain pemerintahan menyarankan perusahaan ini sangat meningkatkan tingkat *IT Governance Maturity*. Penelitian ini berusaha untuk menguji secara empiris lima mekanisme tata kelola TI individu yang mempengaruhi keefektifan tata kelola TI. Penelitian ini meneliti pengaruh dari berikut domain tata kelola TI pada tingkat IT pemerintahan: Penyelarasan Bisnis dan TI (ABIT); Evaluasi Nilai Pengiriman (EVD); Pemantauan IT Sumber daya, Risiko, dan Manajemen (MITRRM); Pemantauan IT Pengukuran Kinerja (MITPM); dan pengembangan *IT Governance* (ITGD).

Nadianatra Musa dan Bob Clift (2013), penelitian ini, untuk mengintegrasikan tiga komponen secara serentak di seluruh IS / IT implementasi keamanan. Model *IS / IT security* pemerintahan adalah kerangka konseptual yang komprehensif karena menekankan hubungan dua arah antara masing-masing komponen. Komponen resmi memiliki interaksi dengan komponen resmi melalui aspek pendidikan. Kebijakan keamanan memiliki interaksi dengan komponen teknis dalam dua cara, sumber daya teknologi dan prosedur keamanan. Sumber daya teknologi difokuskan pada visi IT dan prosedur keamanan yang berkaitan dengan penanggulangan keamanan atau solusi.

Dalam penelitian ini, lebih ditekankan pada penilaian indeks kematangan *IT governance* pada keamanan informasi dengan melihat *Gap Assessment Domain ISMS* nya, sehingga dapat dihasilkan panduan atau pedoman dalam membuat kebijakan dan prosedur untuk mencegah terjadai kebocoran informasi baik dari pihak internal maupun eksternal.

Audit Kemanan Informasi

Audit keamanan informasi adalah suatu alat atau perangkat dalam menentukan, mendapatkan, dan mengelola setiap *level* keamanan dalam suatu organisasi. Audit keamanan informasi dimaksudkan untuk meningkatkan *level* keamanan informasi, mencegah rancangan keamanan informasi yang tidak layak, dan mengoptimalkan efisiensi benteng keamanan, dan proses keamanan informasi itu sendiri. Audit ini akan memastikan atau menjamin berjalannya proses operasional, reputasi dan aset suatu organisasi. Hasil dari audit keamanan informasi adalah tersusunnya dokumen laporan audit yang terkait pada keamanan teknologi informasi yang digunakan di lingkungan organisasi tersebut [2].

Kelemahan keamanan informasi berdasarkan lubang keamanan (*security hole*) dapat diklasifikasikan menjadi empat bagian utama yang akan dijelaskan sebagaimana berikut [3] :

1. Keamanan yang bersifat fisik (*physical security*). Hal tersebut mencakup akses orang ke gedung, peralatan dan media yang digunakan.
2. Keamanan yang berhubungan dengan orang (*personal security*). Hal ini termasuk identifikasi dan profil risiko dari pihak atau karyawan yang mempunyai akses.
3. Keamanan dari data dan media serta teknik komunikasi (*communications security*). Yang termasuk dalam bagian ini adalah kelemahan dalam perangkat lunak (*software*) untuk pengelolaan data.
4. Keamanan dalam operasional/manajemen teknologi informasi *(management security*). Hal ini mencakup kebijakan *(policy*) dan prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan dan juga prosedur setelah serangan *(post attack recover*y), seringkali perusahaan tidak memiliki dokumen kebijakan dan prosedur tersebut**.**

Information Security Management System (ISMS)

Information Security Management System (ISMS) merupakan sebuah kesatuan system yang disusun berdasarkan pendekatan resiko bisnis, untuk pengembangan, implementasi, pengoperasian, pengawasan, pemeliharaan serta peningkatan keamaan informasi perusahaan. Pada tahun 2008 Kementrian Departement Komunikasi dan Informasi Indonesia telah mengeluarkan standar keamanan yang diadopsi dari ISO/IEC 27000 mengenai *Information Security*

Management System (ISMS), yaitu SNI ISO 27000 yang dikenal dengan nama Indeks KAMI [4]. Proses evaluasi Indeks KAMI ini dilakukan dengan 2 metode:

1. Jumlah kelengkapan bentuk pengamanan
2. Tingkat Kematangan proses pengolaan pengamanan informasi Area yang akan diaudit meliputi: Peran TIK di dalam Instansi; Tata Kelola Keamanan Informas; Pengelolaan Risiko Keamanan Informasi; Kerangka Kerja Keamanan Informasi; Pengelolaan Aset Informasi dan Teknologi dan Keamanan Informasi.

ISO/IEC 27001

ISO/IEC 27001 adalah standar information security yang diterbitkan pada October 2005 oleh International Organization for Standarization dan International Electrotechnical Commission. Standar ini menggantikan BS-77992:2002.

ISO/IEC 27001: 2005 mencakup semua jenis organisasi (seperti perusahaan swasta, lembaga pemerintahan, dan lembaga nirlaba). ISO/IEC 27001: 2005 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa dan memelihara seta mendokumentasikan Information Security Management System dalam konteks resiko bisnis organisasi keseluruhan

ISO/IEC 27001 mendefenisikan keperluan-keperluan untuk sistem manajemen keamanan informasi (ISMS). ISMS yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang penting agar terhindar dari resiko kerugian/bencana dan kegagalan serius pada pengamanan sistem informasi, implementasi ISMS ini akan memberikan jaminan pemulihan operasi bisnis akibat kerugian yang ditimbulkan dalam masa waktu yang tidak lama [5].

ISO/IEC 27001 adalah sebuah metode khusus yang terstruktur tentang pengamanan informasi yang diakui secara internasional. Standar ISO/IEC 27001 merupakan dokumen standar sistem manajemen keamanan informasi atau *Information Security Management Syestem*, biasa disebut *ISMS*, yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahan dalam usaha mereka untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi diperusahan berdasarkan "*best practise*" dalam pengamanan informasi [5].

Metode Penelitian

Metodologi penelitian merupakan suatu metode yang digunakan untuk menentukan langkah-langkah yang harus dilakukan dalam sebuah penelitian. Di dalam metodologi penelitian yang harus mencerminkan keterkaitan langkah-langkah sehingga kegiatan menjadi lebih mudah, terarah, dan sistematis. Metode penelitian yang digunakan adalah metode deskriptif dengan pendekatan penelitian kualitatif dan kuantitatif. Sasaran evaluasi penelitian adalah tata kelola TI dalam keamanan layanan informasi adalah STMIK AMIKOM Yogyakarta pada bagian jurusan S1 Teknik Informatika.

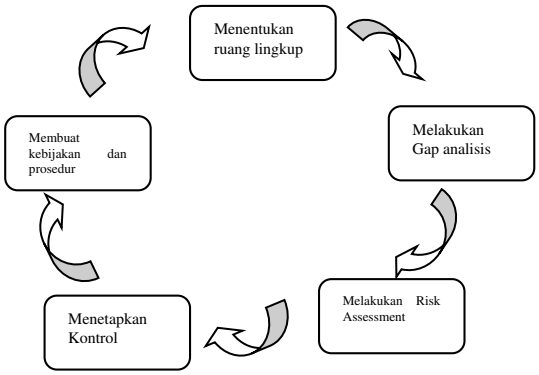
Tahap Evaluasi Kesiapan Keamanan Informasi Pada bagian ini akan dijelaskan mengenai alur pada tahap kedua yaitu tahap evaluasi kesiapan keamanan informasi sebagai berikut :

1. Mendefinisikan ruang lingkup Langkah pertama evaluasi yang harus dilakukan adalah mendefinisikan ruang lingkup penilaian. Ruang lingkup dapat dipilih sesuai dengan kepentingan penilaian Indeks KAMI, dan dapat dipilih sebagai suatu satuan kerja (di tingkat apapun) ataupun suatu sistem informasi.
2. Menetapkan peran atau tingkat kepentingan di instansi Sebelum proses penilaian dilakukan secara kuantitatif, proses klasifikasi dilakukan terlebih dahulu terhadap peran TIK dalam instansi atau cakupan evaluasinya. Responden juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan instansi ke "ukuran" tertentu: Rendah, Sedang, Tinggi dan Kritis.
3. Menilai kelengkapan pengamanan 5 area Penilaian dalam Indeks KAMI dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2009, yang disusun kembali menjadi 5 (lima) area di bawah ini:
   a. Tata Kelola Keamanan Informasi, mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.
   b. Pengelolaan Risiko Keamanan Informasi, mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
   c. Kerangka Kerja Keamanan Informasi, mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
   d. Pengelolaan Aset Informasi, mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut; dan
   e. Teknologi dan Keamanan Informasi, mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan asset informasi.

Hasil Dan Pembahasan

Pemodelan ISMS

Dalam penelitian ini akan menggunakan metode plan pada ISMS, yang memiliki procedural sebagai berikut:



Gambar 1. Proses Plan

Menentukan Ruang Lingkup

Evaluasi terhadap pengendalian sistem informasi akademik sangat memiliki peranan yang sangat penting, karena segala kegiatan operasional yang berkaitan dengan seluruh civitas akademik dapat berjalan secara efektif dan effisien.

Tabel 2. Ruang lingkup manajemen keamanan informasi

No	Data yang dikumpulkan
1	Audit terhadap STMIK AMIKOM yang meliputi: visi, misi serta Mendapatkan *company profile* yang terdiri dari struktur organisasi beserta tugas dan tanggung jawab dan proses sistem informasi yang sedang berjalan saat ini
2	Audit terhadap seluruh asset dalam bentuk teknologi, proses, informasi, jaringan, layanan, system, hardware dan software
3	Risk assessment terhadap keamanan informasi dengan melakukan identifikasi terhadap asset dan ancaman serta menentukan kategori resiko dan menentukan resiko yang di prioritaskan dan monitoring.

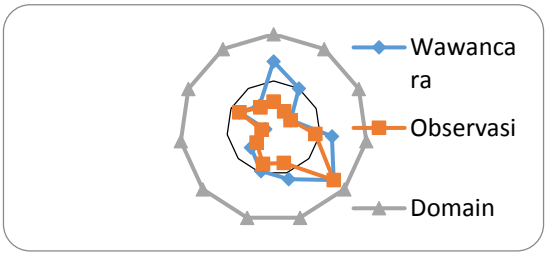
Gap Analisis

Dalam analisis gap ini, digunakan untuk membandingkan terhadap data yang diperoleh dari observasi dan wawancara terhadap responden. Tujuan dari gap analisis ini adalah mengetahui sejauh mana bagian jurusan STMIK AMIKOM dalam menerapkan control-kontrol objek pada ISO 27001 baik meliputi kebijakan, procedure dan dokumen-tasinya.

Tabel 2. Perhitungan Gap Assessment untuk domain ISO 27001

No	Domain	A	B	C	D	E	F	G
1	*Security Policy*	5	2	7	7	0.71	0.28	1
2	*Organization of information security*	6	2,6	12	12	0.5	0.21	1
3	*Asset Management*	4,5	1	5	5	0.2	0.2	1
4	*Human Resources security*	7	5	11	11	0.63	0.45	1
5	*Physical and environmental security*	20,5	18	21	21	0.85	0.85	1
6	*Communication and operations management*	27	18,5	47	47	0.57	0.39	1
7	*Access control*	18	15	37	37	0.48	0.40	1
8	*Information system acquision, development and maintenance*	10	7,5	31	31	0.32	0.24	1
9	*Information security incident management*	1	1,5	11	11	0.09	0.13	1
10	*Business continuity management*	3,5	4	10	10	0.4	0.4	1
11	*comliance*	6	5,5	21	21	0.28	0.26	1

Hasil pada table 2, di sajikan pada gambar Gap assessment berdasarkan wawancara dan observasi dan domain ISMS, bahwa dalam penelitian ini terlihat bahwa di bagian jurusan STMIK AMIKOM masih ada gap sehingga untuk tingkat keamanan informasi masih belum masuk kategori Best Practice.



Gambar 2. Gap Assessment Domain ISMS

Risk Assessment

Dalam tahapan selanjutnya, peneliti akan melakukan risk assessment. Dalam tahapan risk assessment terdiri dari beberapa langkah, meliputi:

1. Melakukan identifikasi asset
2. Melakukan identifikasi kerawanan dan ancaman
3. Menentukan prioritas resiko
4. Mengembangkan control
5. Monitoring

Tahap 1 melakukan identifikasi asset

Dalam identifikasi asset pada STMIK AMIKOM, khususnya pada bagian Jurusan yang berkaitan dengan manajemen keamanan Informasi meliputi:

Tabel 3. Aset keamanan informasi

No	Aset	Pemilik	Alokasi
Aset Perangkat Keras			
1	Server	Inovation Center/IC	Internal
2	Cisco Router	Inovation Center/IC	Internal
3	Digital Video Recorder	Inovation Center/IC	Internal
4	Kamera CCTV	Inovation Center/IC	Internal
5	Access point	Inovation Center/IC	Internal
6	Firewall	Inovation Center/IC	Internal
7	Switch	Inovation Center/IC	Internal
8	PC/Laptop	Kerumahtanggaan	Internal
Perangkat Lunak			
1	OS Windows	Inovation Center/IC	Internal

2	Email	Inovation Center/IC	Internal
3	Anti virus	Inovation Center/IC	Internal
4	Sistem Informasi akademik (Website)	Inovation Center/IC	Internal
Aset Jejaringan			
1	STMIK AMIKOM – Bank Muammallat	*Elektronik Data Processing* (*EDP*)	Internet
Aset Lainnya			
1	Orang	PSDM	Internal

Tahap 2 melakukan identifikasi kerawanan dan ancaman

Setelah melakukan identifikasi asset selesai, tahapan selanjutnya dari penelitian ini adalah melakukan identifikasi terhadap kerawanan (Vulnerability) dan ancaman (Threats) yang terjadi selama ini.

Tabel 4. Hasil identifikasi kerawanan dan ancaman

No	Kerawanan (Vulnerability)	Kode
1	Persyaratan sharing, pengamanan dan pembatasan hak akses	V1
2	Informasi non cetak yang tempat penyimpanannya tidak tepat, misalnya tidak adanya lemari cabinet atau tempat khusus untuk menaruh data file kertas	V2
3	Update yang tidak dilakukan sehingga masih menggunakan versi yang lama	V3
4	Proses maintenance dan monitoring yang tidak dapat berjalan secara berkala dan kurang di pantau	V4
5	Perangkat lunak yang sudah habis lifetimenya dan hardware yang sudah tidak support	V5
6	IP public yang dapat diakses dari jarak jauh	V6
7	Konfigurasi system yang masih bawaan	V7
8	PC belum dilakukan hardening secara tepat dan benar	V8
9	Password yang tidak dig anti secara berkala	V9
No	**Ancaman (Threats)**	**Kode**
1	Serangan virus, worm dan malware	T1
2	Penerobosan/pembobolan system oleh pihak eksternal	T2
3	Penerobosan/pembobolan system oleh pihak internal	T3
4	Adanya Spam pada email	T4
5	Kerusakan software maupun hardware	T5

Tahap 3 melakukan prioritas resiko

Setelah melakukan penentuan criteria tingkat kerawanan dan ancaman, maka akan dilakukan tahapan penentuan prioritas resiko terhadap kerawanan dan ancamana yang terjadi di Jurusan STMIK AMIKOM, meliputi:

1. Mengabungkan antara identifikasi asset dan identifikasi kerawanan dan ancaman,sehingga didapatkan resiko yang mungkin terjadi.
2. Mengkategorikan resiko.
3. Mengidentifikasikan kecenderungan (likehood) dan dampak (impact) dari resiko.
4. Mengidentifikasi inherent risk (risk level sebelum diterapkan control) dan residual risk (risk level setelah diterapkan control).

Menetapkan control

Setelah mengetahui beberapa resiko yang terjadi serta yang harus dilakukan, maka selanjutnya melakukan control untuk mengurangi resiko dengan melakukan penetapan control dari hasil identifikasi kerawanan, dan ancaman yang disajikan pada table berikut.

Tabel 5. Kontrol ISO 27001 untuk kerawanan

No	Kerawanan	Kontrol ISO	Rencana Kerja	Kode
1	Persyaratan sharing, pengamanan dan pembatasan hak akses	*User responsibilities*	Melakukan monitoring dan sosialisasi pengguna dengan mengikuti peraturan yang ditetapkan	RK-V1
2	Informasi non cetak yang tempat penyimpanannya tidak tepat, misalnya tidak adanya lemari cabinet atau tempat khusus untuk menaruh data file kertas	*Media handling*	Pengamanan data dan file, yang berbentuk softcopy diberikan security dan hardcopy di simpan dilemari cabinet dengan pengamanan	RK-V2
3	Update yang tidak dilakukan sehingga masih menggunakan versi yang lama	*System planning and acceptance*	Melakukan pengupgradetan system secara berkala serta pengujian system apakah sudah berjalan dengan baik	RK-V3
4	Proses maintenance dan monitoring yang tidak dapat berjalan secara berkala dan kurang di pantau	*Monitoring*	Menetapkan posedur dan pemantauan dalam penggunaan fasilitas informasi dan sistem	RK-V4
5	Perangkat lunak yang sudah habis lifetimenya dan hardware yang sudah tidak support	*Security of System files*	Membuat prosedur, pemantauan dan pengendalian terhadap fasilitas	RK-V5
6	IP public yang dapat diakses dari jarak jauh	*Network access control, mobile computing and teleworking, terminating or change employement*	Mengidentifikasi terhadap user, membuat kebijakan dan pembatasan hak akses	RK-V6
7	Konfigurasi system yang masih bawaan	*Application and information access control*	Membuat konfigurasi dan pembatasan terhadap system aplikasi sesuai dengan prosedur yang berlaku	RK-V7
8	PC belum dilakukan hardening secara tepat dan benar	*Network Access control*	Melakukan pengendalian kases secara fisik dan logical	RK-V8
9	Password yang tidak diganti secara berkala	*User access management*	Pemantauan hakses dan pembatasan hak akses	RK-V9

Menetapkan Kebijakan dan Prosedur

Hasil dari pemetaan terhadap kerawanan dan ancaman dengan menggunakan control ISO 27001,

maka akan dijabarkan beberapa kebijakan dan prosedur dalam menanggani hal tersebut yang disajikan pada table berikut ini.

Tabel 6. Kebijakan, procedure, dokumentasi dan instruksi

No	Kontrol ISO 27001	Kebijakan, prosedur, dokumentasi dan instruksi
1	*User responsibilities*	1. User melakukan instruksi dengan meng logout system saat ditinggal sehingga informasi akan aman 2. Membuat prosedur dengan menggantikan password secara berkala untuk menghindarkan pembobolan oleh pihak lain 3. Membuat suatu instruksi clear desk maupun screen dengan media penyimpanan yang tepat untuk menjaga kerapian dan keamanan
2	*Media handling*	1. Membuat prosedur cara penyimpanan dan penanganan dokumen, baik melalui harddisk maupun lemari kabinet 2. Membuat suatu prosedur terhadap pemusnahan data atau informasi yang sudah tidak digunakan untuk menjaga keamanan 3. Pembuatan dokumentasi terhadap penggunaan hak akses untuk bias dilakukan monitoring oleh lembaga
3	*System planning and acceptance*	1. Pembuatan dokumentasi terhadap penggunaan system baru, upgrade serta melakukan penguji terhadap system 2. Pembuatan dokumentasi terhadap pengadaan dan pemenuhan terhadap kapasitas dalam mendukung kinerja system 3. Pembuatan procedure dalam melakukan pengembanagan dan pengelolahan sistem
4	*Monitoring*	1. Membuat dokumentsi melakukan audit terhadap asset 2. Membuat prosedur dalam melakukan pemantauan secara berkala 3. Pembuatan dokumentsi terhadap pengamanan dan penagangganan suatu system 4. Pembuatan dokumentasi terhadap penggunaan hak akses
5	*Security of System files*	1. Pembuatan prosedur terhadap pengamanan data dan informasi pada system 2. Pembuatan prosedur hak akses
6	*Network access control, mobile computing and teleworking, terminating or change employement*	1. Membuat kebijakan dalam pengaturan tentang pembagian jaringan 2. Membuat kebijakan dalam melakukan pembagian hak akses 3. Membuat procedure dalam melakukan identifikasi peralatan yang digunakan secara spesifik
7	*Application and information access control*	1. Membuat kebijakan dalam penggunaan fasilitas mobile dalam melindungi informasi dalam menghindari terjadi resiko 2. Membuat procedure dalam melakukan pemamntauan hak akses dengan mobile
8	*User access management*	1. Pembuatan procedure dalam pendaftaran hak akses dan penghapusan hak akses 2. Pembuatan procedure pembagian hak akses 3. Pembuatan kebijakan pengantian password dan menjaga rahasia terhadap password yang digunakan
9	*Reporting information security events and weakness*	1. Pembuatan dokumentasi dalam pelaporan terjadinya insiden proses keamanan informasi 2. Pembuatan dokumentasi terhadap kelemahan system yang mengalami insiden
12	*Exchange of information*	1. Pembuatan procedure dalam melakukan pengendalian dan keamanan informasi 2. Pembuatan procedure dalam melakukan pengamanan jaringan 3. Pembuatan procedure dalam penggunaan hak akses untuk melindungi keamanan informasi
13	*Equipment security*	1. Pembuatan procedure dalam melakukan pengamanan aset baik berbentuk perangkat lunak maupun keras 2. Pembuatan procedure dalam pengendalian kerusakan oleh pihak internal maupun eksternal

Kesimpulan dan Saran

1. Jurusan STMIK AMIKOM memiliki kekurangan pada keamanan informasi disebabkan karena belum adanya kontrol, aturan, kebijakan, standar untuk perlindungan keamanan informasi.
2. Belum adanya pencatatan maupun dokumentasi secara berkala mengenai insiden kelemahan keamanan informasi yang disebabkan karena tidak terdapat kebijakan, prosedur maupun aturan untuk menang-gulangi insiden kelemahan terhadap keamanan informasi. Hal ini dapat dilihat dalam pembahasan keamanan informasi dalam melakukan kontrol akses, dan akuisis sistem infomasi, tidak ada kontrol untuk mengatasi masalah ini dan kurangnya pendokumentasian prosedur, kebijakan dan peraturan.

Dalam hal ini, peneliti memberikan beberapa saran demi kemajuan dalam penelitian ini adalah:

1. Perlu adanya dokumentasi dan prosedur yang harus di buat oleh lembaga dalam menerapkan manajemen keamanan informasi dalam pelayanan.
2. Perlu adanya penilaian yang lain dalam menilaia manajemen keamanan informasi selain menggunakan ISMS dengan domain ISO 27001.

Daftar Pustaka

[1] Surendro, Kridanto. (2009). Implementasi Tata Kelola Teknologi Informasi. Bandung: Informatika Bandung.

[2] Kemenpora. (2012). *Bakuan Audit Keamanan Informasi Kemenpora.* Jakarta: Kementrian Pemuda dan Olahraga Republik Indonesia.

[3] Sarno, Riyanarto dan Irsyat Iffano.(2009). *Sistem Manajemen Keamanan Informasi.* Surabaya: ITSPRess.
[4] Tim Direktorat Keamanan Informasi Depkominfo. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik.
[5] ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management System – Requirements, 15 Oktober 2005
[6] Kusumah, P.; Sutikno, S.; Rosmansyah, Y. 2014. Model design of information security governance assessment with collaborative integration of COBIT 5 and ITIL (case study: INTRAC). ICT For Smart Society (ICISS), 2014 International Conference on 2014. Pages: 1 - 6, DOI: 10.1109/ICTSS.2014.7013193. IEEE Conference Publications.
[7] Budi Yuwono and Annas Vijaya. 2011. The Impact of Information Technology Governance Maturity Level on Corporate Productivity: a Case Study at an Information Technology Services Company. ICACSIS 2011 ISBN: 978-979-1421-11-9 Advanced Computer Science and Information System (ICACSIS), 2011 International Conference on 2011. Pages: 291 – 296. IEEE Conference Publications.
[8] Humam AlAgha. 2013. Examining the Relationship between IT Governance Domains, Maturity, Mechanisms, and Performance: An Empirical Study toward a Conceptual Framework 2013 10th International Conference on Information Technology: New Generations. 978-0-7695-4967-5/13 $26.00 © 2013 IEEE DOI 10.1109/ITNG.2013.122
[9] Nadianatra Musa and Bob Clift. 2013. A model of component interaction between Formal, Technical and Informal components within IS/IT security governance. The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013). 978-1-908320-20 IEEE