Applied Information Systems and Management (AISM)
Volume 1, (2) 2018, hal 108-116
P-ISSN: 2621-2536; E-ISSN: 2621-2544

Usulan Evaluasi Sistem Keamanan Informasi Berdasarkan Standar ISO/IEC 27002:2013 pada Pondok Pesantren Kafila *International Islamic School* Jakarta

Aditya Teguh Septoaji[1], Fitroh[2], Elsy Rahajeng[3]

***Abstrak*— Kafila International Islamic School (KIIS) adalah sebuah pesantren *(boarding school)* yang mempunyai banyak prestasi di beberapa perlombaan dan nilai Ujian Nasional. Sejak 2007, KIIS sudah menerapkan standar ISO 9001:2008 sebagai standar mutu pendidikan. Namun, dengan penerapan ISO 9001:2008 belum menutup semua celah baik kelemahan *(vulnerable)* atau ancaman *(threat)* yang timbul ketika proses pembelajaran sekolah berlangsung. Dalam wawancara penulis, KIIS memerlukan solusi untuk improvisasi keamanan dan dokumentasi yang lebih baik terutama dalam fasilitas informasi, yaiu dengan melakukan penelitian evaluasi menggunakan ISO 27002:2013, penelitian Keamanan Sistem Informasi ini dilakukan pada 8 klausul, pada kebijakan keamanan informasi, keamanan informasi organisasi, keamanan sumber daya (pekerjaan), manajemen aset, kontrol akses, keamanan fisik dan lingkungan, keamanan operasi, akusisi sistem informasi, pembangunan dan pemeliharaan). Dalam penelitian ini, penulis menggunakan metode pengukuran kapabilitas tingkat kedewasaan (CMM). Dapat dihasilkan nilai kedewasaan 4 *(managed)* pada klausul kebijakan keamanan informasi, keamanan informasi organisasi, keamanan sumber daya dan manajemen aset. Selanjutnya Nilai kedewasaan 3 *(defined)* pada klausul Kontrol Akses, Keamanan fisik dan lingkungan, Keamanan operasi, Akusisi sistem informasi dan pembangunan dan pemeliharaan.**

***Kata Kunci*— Sekolah, Keamanan Sistem Informasi, ISO 272002**

I. PENDAHULUAN

Penggunaan teknologi informasi di berbagai organisasi saat ini sangat dibutuhkan untuk mempermudah melakukan pendataan dan pengambilan keputusan yang strategis[1]. Perkembangan teknologi informasi pada saat ini menyebabkan perubahan peran teknologi informasi bagi organisasi, teknologi informasi tidak hanya difungsikan sebagai pendukung *(support)* tetapi menjadi bagian dari organisasi dalam mecapai kesuksesan [2]. Organisasi-pun pada hampir semua sektor membutuhkan teknologi, terutama teknologi informasi untuk setiap sistem informasi mereka. Bahkan bisa dikatakan, "teknologi informasi acapkali tidak dapat dipisahkan dengan keperluan bisnis" [3].

Perkembangan Teknologi Informasi saat ini tidak hanya berfungsi sebagai penyedia jasa layanan saja[4], melainkan diharapkan dapat berperan menjadi partner dalam menentukan strategi bisnis baru. Maka perlu memperhatikan bagaimana tata kelola teknologi informasi supaya proses berjalannya teknologi informasi dapat berjalan secara optimal dalam mendukung strategi bisnis [5].

Informasi adalah aset dalam bisnis. Karena sifatnya yang penting, maka perlu di proteksi [6]. Informasi dapat disimpan dalam berbagai macam media, seperti: media digital dan media cetak. Informasi dapat dikirim menggunakan kurir, elektronik hingga komunikasi verbal. Apapun cara penyimpanannya dan cara penyebarannya, tetap diperlukan keamanan untuk menjamin terjaganya informasi [6]. Menurut laporan Symantec (2015), tercatat 312 pelanggaran keamanan informasi dan mengakibatkan kerugian senilai 348 juta dikarenakan terbongkarnya informasi pribadi, seperti data kartu kredit, data riwayat medis, data pribadi, ID *login*, dan lainnya[7]. Aspek Keamanan Informasi sangat penting, terutama dalam aspek pelayanan fasilitas pendidikan, karena secara tidak langsung mempengaruhi *"income"* dan *"outcome"* dalam bisnis prosesnya [8].

Peneliti mengadakan wawancara dengan beberapa *stakeholder* [9] IT KIIS, wawancara pertama kepada Direktur Pendidikan KIIS, Bapak Achmad Alwasim. Beliau bahwa KIIS berencana pada Juli 2019, Kafila akan memperbaharui ISO 9001. Dari ISO 9001:2008 ke ISO 9001:2015. Hasil dari penelitian ini diharapkan dapan menambah nilai mutu untuk administrasi Pendidikan yang lebih baik untuk KIIS. Kemudian ke divisi IT bidang Alquran, menurut Bapak Abdurrohim, Admin Bidang Alquran KIIS dan sekaligus penanggungjawab aplikasi TahfizApp, perlu pedoman alur dan struktur data yang tepat dalam perancangan dan pembuatan aplikasi [10], karena

Received: 16 Juli 2018; Revised: 20 Agustus 2018; Accepted: 1 September 2018.

A. T. Septoaji, *staf IT di Kafila Internasional Islamic School* (adityat626@gmail.com)
Fitroh, *dosen Prodi Sistem Informasi UIN Syarif Hidayatullah Jakarta* (fitroh@uinjkt.ac.id)
E. Rahajeng, *dosen Prodi Sistem Informasi UIN Syarif Hidayatullah Jakarta* (elsy.rahajeng@uinjkt.ac.id)

pada ujian *tahfidz* semester 1 tahun 2019 misalnya, ada beberapa ujian yang gagal dikarenakan kesalahan tipe data (NaN) dalam pemrosesan *input*.

Wawancara dilanjutkan dengan Bapak Rifki Baisa, staf labkom spesialis jaringan. Beliau menghimbau perlu adanya pengaturan kebijakan penataan teknologi dan pencatatan aset-aset jaringan dan CCTV *(control room)*, sering terjadi kehilangan dan kerusakan aset dan tidak terdokumentasikan dengan baik [11].

Berikutnya adalah wawancara kepada Bapak Taufiqurrohman. Sebagai kepala Laboratorium Komputer KIIS. Kepala Laboratorium Komputer (labkom) mempunyai tanggung jawab untuk pemeliharaan data dan pengembangan sistem aplikasi digital yang kini sudah berjalan di KIIS. Namun, faktor dokumentasi untuk regenerasi penerus pengurus perlu dipertimbangkan. Mengingat proses regenerasi adalah proses *transfer knowledge*. Beliau menambahkan, ISO 9001 (yang sudah dilengkapi ISO 31000) mengenai manajemen mutu sudah dirasa cukup untuk pengendalian mutu laboratorium, namun masih ada kekurangan dalam dokumentasi Aset IT. Pada 20 Januari 2020, terjadi kehilangan data pada server sekolah (salah satu hardisk RAID server mati) dikarenakan tidak berjalannya fungsi pengecekan pada aset-aset di KIIS.

Semua masalah yang telah terjadi bukan hanya karena upaya tindakan yang kurang baik, tetapi karena belum adanya standar dari prosedur keamanan yang ada, standar operasional prosedur yang belum memenuhi standar keamanan, bahkan ada beberapa standar operasional prosedur yang mengambil dari sumber internet dan belum mengadaptasi dengan lingkungan keamanan informasi. Dari hasil wawancara tersebut, diperlukan evaluasi pada perangkat (aset) IT pada KIIS.

II. KAJIAN PENELITIAN

A. Sistem

Sistem merupakan kumpulan elemen/fungsi yang saling terhubung satu sama lain yang membentuk kesatuan dalam mencapai tujuan yang sama [12].

B. Informasi

Ref. [12] menguraikan, bahwa informasi adalah data yang telah diklasifikasi (disekat) kemudian dipakai sebagai bahan dalam pengambilan keputusan (*decision*).

C. Sistem Informasi

Sistem Informasi adalah suatu sistem di dalam organisasi/perusahaan yang mendukung fungsi operasi organisasi (harian, pekanan hingga rekayasa manajemen lainnya) yang bersifat manajerial untuk dapat menyediakan informasi yang berguna kepada pihak luar tertentu dengan laporan-laporan [12].

D. Keamanan Informasi

Dalam keamanan informasi, ancaman *(threat)* adalah setiap kegiatan yang dapat membahayakan informasi. Ancaman ini kerapkali akan menjadi negatif jika menguak *(leaking)* dan memanipulasi kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan *(availability)* dari sebuah sistem [13].

E. Sistem Manajemen Keamanan Informasi

Keberadaan dokumen "Kebijakan Keamanan" atau *"Security Policies"* merupakan sebuah infrastruktur keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi terpentingnya. Dokumen ini berisikan tata cara mengamankan informasi, baik secara langsung maupun tidak langsung [14].

III. METODE PENELITIAN

A. Metode Pengumpulan Data

1) Kuesioner

Pengumpulan data dilakukan dengan menggunakan kuesioner [15]. Narasumber yang penulis pilih adalah Kepala HRD, Kepala Labkom dan Kepala Logistik KIIS. Penulis menggunakan metode kuesioner personal (ahli) dan diisi langsung oleh responden sesuai dengan keadaan sebenar-benarnya.

2) Wawancara

Wawancara penulis lakukan dengan Direktur Pendidikan Kafila *International Islamic School* yang merupakan pemimpin organisasi KIIS.

B. Metode Analisis Data

1) Plan, pada tahap ini, peneliti menemui Direktur Pendidikan Kafila *International Islamic School*, mempelajari kembali profil, visi dan misi hingga struktur transformasi terbaru Kafila *International Islamic School*.

2) Do, peneliti mengamati secara langsung bagaimana manajemen berjalan pada Kafila International Islamic School. Proses yang dilakukan adalah mengidentifikasi risiko, langkah dalam indentifikasi risiko adalah sebagai berikut: Identifikasi aset pada Kafila *International Islamic School*. Parameter identifikasi adalah kerahasiaan informasi, keutuhan informasi dan ketersediaan informasi (CIA *triad*).

a) Identifikasi pada proses bisnis yang berjalan dan akan berjalan pada aspek ancaman dan kelemahan.

b) Menganalisa dan evaluasi risiko, merupakan tindak lanjut dari identifikasi risiko. Penulis menganalisa risiko, apakah risiko dapat diabaikan ataukah harus dilakukan tindakan preventif untuk menghindari risiko tersebut. Langkah yang penulis lakukan adalah:

(1) Menganalisa dampak bisnis. Penulis menggunakan metode *Bussiness Impact Analysis* (BIA) dalam penentuan skala.
(2) Membuat matriks level risiko untuk menganalisa risiko yang terjadi dan akan terjadi sehingga nilai dari matriks ini menjadi perhatian dalam menentukan rencana kedepannya.
(3) Jika sudah ditentutan matriksnya, diberikan prioritas pengelolaan risiko dari prioritas tinggi (darurat) hingga prioritas rendah

3) Check, proses pengecekan ini adalah pemilihan obyek kontrol dan kontrol keamanan informasi berdasarkan kondisi dan nilai risiko yang didapat dari langkah sebelumnya (matriks

level risiko). Penulis juga mengukur kematangan keamanan sistem. Langkah penilaian kematangan sistem sebagai berikut:
Kuesioner, diberikan kepada 3 bagian penting organisasi:

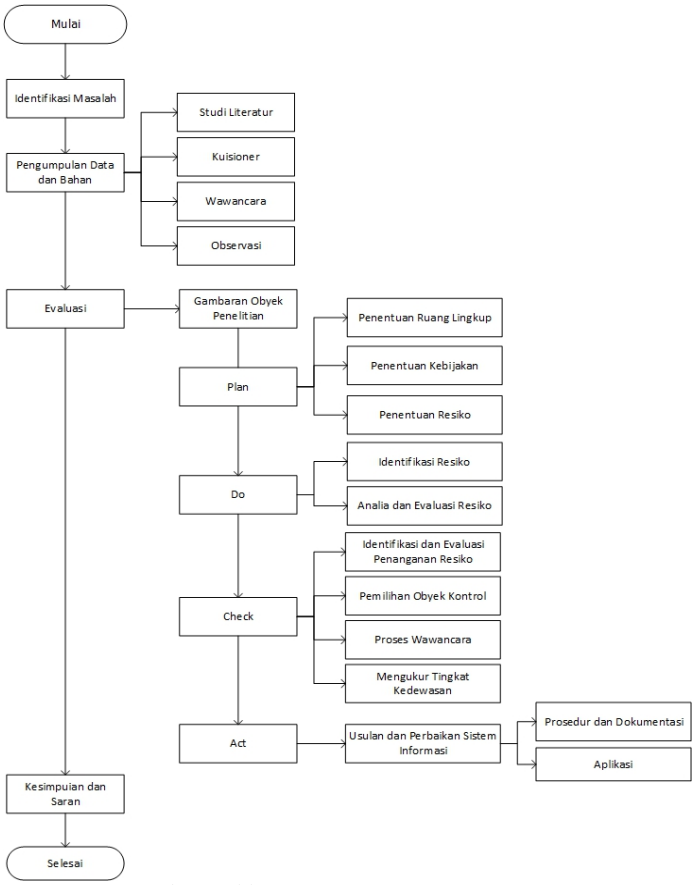
a) Manajemen Representatif, Kepala Labkom, Koordinator Jaringan dan Staf Labkom dengan jumlah responden sebanyak 4 orang.
b) Penilaian tingkat kematangan system, menggunakan *Security Engineering Capability Maturity Level* (SSE-CMM). Penjelasan penilain adalah seperti pada Tabel 1.

Tabel 1.
Tingkat Kemampuan SSE-CMM

Rentang Nilai	Tingkat Kematangan
0 – 0,50	0 – *Non Existent*
0,51 – 1,50	1 – *Initial*
1,51 – 2,50	2 – *Repeteable*
2,51 – 3,50	3 – *Defined*
3,51 – 4,50	4 – *Managed*
4,51 – 5,00	5 – *Optimized*

Penghitungan yang dipakai adalah nilai hasil level kematangan rata-rata dari setiap kontrol obyek dan rata-rata keseluruhan klausul.

1. *Act*, penulis memberikan rekomendasi dari hasil temuan penghitungan nilai kematangan yang sudah dihitung sebelumnya sebagai bahan evaluasi proses bisnis Kafila International Islamic School.



Gambar 1. Kerangka Peneitian

IV. HASIL

A. Plan

1) Identifikasi Aset

Tabel 2. Identifikasi Aset

Infrastruktur IT di KIIS	
Location	Jalan Raya Bogor KM 22,5 Ciracas Jakarta Timur
Business Application	Myschool (akademik), Ehsan *(feedback)*, TahfizApp (alquran)
Operating System Services	Server: Redhat *Desktop*: Windows 7 dan Windows 10
Network Services	*Email* & Pop
Security	*Firewall: default*
Communication Infrastructure	LAN, WAN, Mikrotik

Tabel 3. Spesifikasi Aset IT KIIS

Spesifikasi Aset IT KIIS	
Server	IBM System x3650 (2016) *Operating System*: Redhat RHEL 7.4 (2017) *Firewall: firewall (default)*
Labkom *Backup Computer* (*Server*)	*Operating System*: Windows 10, Intel i5 (5th Generation), 8 GB RAM
Labkom *Backup Computer* (MTS)	*Operating System*: Windows 7 SP1, Intel i5 (5th Generation), 8 GB RAM
Labkom *Backup* Computer (MA)	*Operating System*: Windows 8, Intel i5 (5th Generation), 8 GB RAM
Labkom *Computer* (*Students*)	*Operating System*: Xubuntu vers 20, Intel i5 (5th Generation), 4-8 GB RAM
Network	OS: Mikrotik Vers 6.34 (*updated* Maret 2016)
Switch LAN-hub	TP LINK TL-SG1024D (24 PORT) -> Labkom, D-Link DES 1024D (24 Port) -> *Control Roo*m
Wifi *Router*	Tp-link TL-WR840N, Ubiquity N2

2) Penentuan Resiko

a. Metode Risk Assessment

Metode yang penulis lakukan dalam penilaian resiko adalah metode matematis dengan penerapan logika.

b. Kriteria Penerimaan Resiko

Tabel 4. Kriteria Penerimaan Resiko

Penerimaan Resiko	Keterangan
Resiko Diterima *(risk acceptable)*	Resiko dapat diterima organisasi dengan segala dampaknya dan proses bisnis dapat berjalan terus
Resiko direduksi *(risk reduction)*	Resiko dapat diterima organisasi, namun organisasi mereduksi dampaknya dengan menggunakan kontrol keamanannya
Resiko dihindari atau ditolak *(risk avoidance)*	Organisasi perlu menghindari penyebab penyebab timbulnya resiko dan menghentikan aktifitasnya jika gejala resiko muncul seperti mematikan manual komputer server jika tidak dapat dimatikan melalu command promp/terminal komputer *backup server*
Resiko dialihkan pada pihak ketiga *(risk transfer)*	Organisasi menerima resiko tersebut dengan mengalihkan kepada pihak ketiga dengan kompensasi sesuai perjanjian dengan perusahaan seperti: vendor asuransi, garansi prosuk dan lainnya.

3) Tabel Aset Informasi KIIS

Tabel 5. Aset Informasi KIIS

Jenis Aset	Nama Aset	Penjelasan
Dokumen	Data Karyawan	Guru dan pegawai KIIS.
	Data PSB	Siswa saat baru mendaftar
	Data Sekolah	Dokumentasi pembelajaran.
	Data Keasramaan	Dokumentasi keasramaan.
	Data *Tahfidz*	Dokumentasi tahfidz.
Perangkat Lunak Sistem	Data Laboratorium Komputer	Berbagai aplikasi di kembangkan di labkom.
	Aplikasi MySchool	digunakan untuk mengeola data sekolah
	Aplikasi PSB	digunakan untuk mengeola data siswa baru
	Aplikasi Ujian Quran	digunakan untuk ujian quran
	Aplikasi Asrama	digunakan untuk pengelolaan asrama
Perangkat Keras	Laboratorium	digunakan siswa dalam proses KBM TIK
	Mikrotik	Jaringan Internet dan LAN KIIS
	Server	alat penyimpanan aplikasi dan data lokal
	Komputer Backup Server	backup server
	Komputer Asrama	bidang asrama
	Komputer Tahfidz	bidang tahfidz
	Komputer Admin	pengelolaan data surat menyurat KIIS hingga pengelolaan data pegawai
	CCTV Labkom	CCTV keamanan
	Pemadam Kebakaran	Fitur dalam gedung sebagai detektor panas dan asap, bel darurat, dan alat pemadam kebakaran
	Pendingin Ruangan (AC)	*online* 24 jam

4) Perhitungan Nilai Aset

Tabel 6. Nilai Aset

Jenis Aset	Nama Aset	NC	NI	NV	NA
Dokumen	Data Karyawan	4	3	2	9
	Data Penerimaan Siswa Baru	4	3	2	9
	Data Sekolah	4	4	4	12
	Data Keasramaan	4	3	4	11
	Data Tahfidz	4	3	4	11
Perangkat Lunak Sistem	Data Laboratorium Komputer	4	4	4	12
	Aplikasi MySchool	4	4	4	12

Perangkat Keras	Aplikasi PSB	4	2	4	10
	Aplikasi Ujian Quran	4	2	2	8
	Aplikasi Asrama	4	3	4	11
	Komputer Laboratorium	2	3	3	8
	Mikrotik	4	4	4	12
	Server	4	4	4	12
	Komputer *Backup Server*	4	2	2	8
	Komputer Asrama	4	3	3	10
	Komputer Tahfidz	3	3	2	8
	Komputer Admin	4	4	4	12
	CCTV Labkom	4	4	4	12
	Pendingin Ruangan (AC) Labkom	4	1	4	9
	Pemadam Kebakaran (*fire extinguisher* dan sensor api dalam gedung)	2	2	4	8

5) Identifikas Ancaman

Tabel 7. Identifikasi Ancaman

Nama Aset	Nilai Aset	Nilai Ancaman	Status
Data Karyawan	9	0,46	*Medium*
Data PSB	9	0,46	*Medium*
Data Sekolah	12	0,46	*Medium*
Data Keasramaan	11	0,46	*Medium*
Data Tahfidz	11	0,46	*Medium*
Data Laboratorium Komputer	12	0,46	*Medium*
Aplikasi MySchool	12	0,55	*Medium*
Aplikasi PSB	10	0,55	*Medium*
Aplikasi Ujian Quran	8	0,55	*Medium*
Aplikasi Asrama	11	0,55	*Medium*
Mikrotik	12	0,6	*Medium*
Server	12	0,5	*Medium*
Komputer Laboratorium	8	0,42	*Medium*
Komputer Backup Server	8	0,47	*Medium*
Komputer Asrama	10	0,42	*Medium*
Komputer Tahfidz	8	0,42	*Medium*
Komputer Admin	12	0,42	*Medium*
CCTV Labkom	12	0,6	*Medium*
AC	9	0,56	*Medium*
Fire Extinguisher	8	0,6	*Medium*

Dengan kriteria penilaian sebagai berikut:
Low = Nilai Rerata 0,1 – 0,3
Medium = Nilai Rerata 0,4 – 0,6
High = Nilai Rerata 0,7 – 1,0

B. Do

1) Analisa dan Evaluasi Resiko

a) Analisa Dampak Bisnis

Tabel 8. Nilai BIA

Fasilitas Informasi	Impact	Nilai BIA	Status
Data Karyawan	Data Hilang	85	*Very high critical*
Data Penerimaan Siswa Baru	Data Hilang	25	*Minor critical*
Data Sekolah	Data Hilang	90	*Very high critical*
Data Keasramaan	Data Hilang	90	*Very high critical*
Data Tahfidz	Data Hilang	90	*Very high critical*
Data Laboratorium Komputer	Data Hilang	25	*Minor critical*
Aplikasi MySchool	Aplikasi tidak dapat digunakan	100	*Very high critical*
Aplikasi PSB	Aplikasi tidak dapat digunakan	40	*Minor critical*
Aplikasi Ujian Quran	Aplikasi tidak dapat digunakan	70	*High critical*
Aplikasi Asrama	Aplikasi tidak dapat digunakan	100	*Very high critical*
Mikrotik	Jaringan Terputus	100	*Very high critical*
Server	Operasi terhenti	100	*Very high critical*
Komputer Laboratorium	Operasi terhenti	50	*Mayor critical*
Komputer Backup Server	Operasi terhenti	80	*High critical*
Komputer Asrama	Operasi terhenti	100	*Very high critical*
Komputer Tahfidz	Operasi terhenti	80	*Very high critical*
Komputer Admin	Operasi terhenti	95	*Very high critical*
CCTV Labkom	Operasi terhenti	90	*Very high critical*
Pendingin Ruangan (AC) Labkom	Operasi terhenti	95	*Very high critical*
Fire Extinguisher	Terjadi Kebakaran	90	*Very high critical*

2) Mengestimasi Level Resiko

Setelah ditemukannya nilai aset, nilai ancaman (NT) dan nilai BIA, maka kita dapat menimbang level resiko masing-masing aset informasi di Kafila International Islamic School. Namun sebelum perhitungan dimulai, terlebih dahulu

penulis membuat matriks level resiko yang variabelnya diambil dari variabel nilai aset, nilai ancaman dan nilai BIA

3) Menentukan Penerimaan Resiko

Penulis menilai resiko berdasarkan hitungan menggunakan metode matematis sebagai berikut;

Tabel 9. Pengukuran Tingkat resiko

Nama Aset	Nilai Aset	BIA	Nilai Ancaman	*Risk Value*	Status
Data Karyawan	9	85	0,46	496,8	*High Risk*
Data Penerimaan Siswa Baru	9	25	0,46	455,4	*High Risk*
Data Sekolah	12	90	0,46	455,4	*High Risk*
Data Keasramaan	11	90	0,46	138	*High Risk*
Data Tahfidz	11	90	0,46	660	*High Risk*
Data Laboratorium Komputer	12	25	0,46	220	*High Risk*
Aplikasi MySchool	12	100	0,55	308	*High Risk*
Aplikasi PSB	10	40	0,55	605	*High Risk*
Aplikasi Ujian Quran	8	70	0,55	720	*High Risk*
Aplikasi Asrama	11	100	0,55	600	*High Risk*
Mikrotik	12	100	0,6	168	*High Risk*
Server	12	100	0,5	300,8	*High Risk*
Komputer Laboratorium	8	50	0,42	420	*High Risk*
Komputer Backup Server	8	80	0,47	268,8	*High Risk*
Komputer Asrama	10	100	0,42	478,8	*High Risk*
Komputer Tahfidz	8	80	0,42	648	*High Risk*
Komputer Admin	12	95	0,42	478,8	*High Risk*
CCTV Labkom	12	90	0,6	432	*High Risk*
AC	9	95	0,56	496,8	*High Risk*
Fire Extinguisher	8	90	0,6	455,4	*High Risk*

C. Check

1) Identifikasi dan Evaluasi Pilihan Penanganan Resiko

Setelah penulis melakukan analisa dan evaluasi resiko apasaja yang kerap mungkin terjadi pada fasilitas IT KIIS, berikut penanganan resiko yang dapat direncanakan:

a) Apabila hasilnya "diterima", maka perlu menerapkan kontrol keamanan yang sesuai.

b) Apabila hasilnya direduksi, hampir sama dengan poin 1, dengan beberapa penambahan pasal untuk keamanan.

c) Resiko yang dapat ditransfer kepada pihak ketiga, akan diatur juga dalam pasal poin 1.

2) Pemilihan Obyek Kontrol dan Kontrol untuk Pengelolaan Resiko

Dengan adanya beberapa kerentanan dalam data, aplikasi dan fasilitas fisik IT, maka penulis menemukan kontrol obyek dalam ISO 27002 yang berhubungan sesuai dengan dokumentasi ISO 27002:2013 (BSI, 2013) , yaitu: *Information security policies* (klausul 5), *Organizational of information security* (klausul 6), *Human resource security* (klausul 7), *Asset management* (klausul 8), *Access control* (klausul 9), *Physical and environment security* (klausul 11), *Operation security* (klausul 12), dan *System acquisition development and maintenance* (klausul 14).

3) Wawancara

Tabel dibawah menunjukkan bagian yang akan diwawancara berdasarkan klausul yang telah ditentukan:

Tabel 10. Narasumber

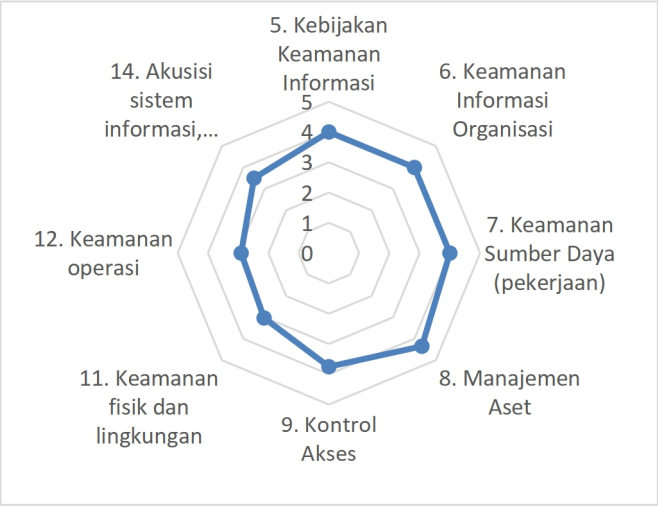
Klausul	Deskripsi	Bagian
5	Kebijakan keamanan informasi	
6	Keamanan Informasi Organisasi	HRD
7	Keamanan Sumber Daya	
8	Manajemen Aset	Kepala Sarana dan Prasarana
9	Kontrol Akses	Kepala Labkom
11	Keamanan fisik dan lingkungan	Kepala Sarana dan Prasarana
12	Keamanan operasi	Kepala Labkom
14	Akusisi sistem informasi, pembangunan dan pemeliharaan	Kepala Sarana dan Prasarana

D. Act, Usulan Perbaikan Sistem Informasi

Berikut adalah perolehan dari seluruh Klausul:

Tabel 11. Nilai Kematangan Seluruh Klausul

Klausul	Maturity Level
5. Kebijakan Keamanan Informasi	4
6. Keamanan Informasi Organisasi	4
7. Keamanan Sumber Daya (pekerjaan)	4
8. Manajemen Aset	4,35
9. Kontrol Akses	3,75
11. Keamanan fisik dan lingkungan	3,03
12. Keamanan operasi	2,9
14. Akusisi sistem informasi, pembangunan dan pemeliharaan	3,5



Gambar 2. Hasil Tingkat Kematangan dari Seluruh Klausul

Berikut adalah representasi dari hasil *maturity level* seluruh klausul.

1) Pada klausul 5, KIIS memperoleh nilai maturity level sebesar 4 dan berada pada tingkat *managed*.

2) Pada klausul 6, KIIS memperoleh nilai *maturity level* sebesar 4 dan berada pada tingkat *managed*.

3) Pada klausul 7, KIIS memperoleh nilai *maturity level* sebesar 4 dan berada pada tingkat *managed*.

4) Pada klausul 8, KIIS memperoleh nilai *maturity level* sebesar 4,35 dan berada pada tingkat *managed*.

5) Pada klausul 9, KIIS memperoleh nilai *maturity level* sebesar 3,75 dan berada pada tingkat *managed*.

6) Pada klausul 11, KIIS memperoleh nilai *maturity level* sebesar 3,03 dan berada pada tingkat *defined.*

Berikut adalah beberapa rekomendasi yang dapat disimpulkan oleh penulis sebagai *best practice* dalam perbaikan keamanan informasi pada Kafila International Islamic School.

1) Prosedur dan Dokumentasi

Berikut adalah rekomendasi penulis mengenai klausul yang bermasalah sesuai pada *best practice* ISO 27002:

a) Klausul 6.2 Pada Perangkat Seluler dan Teleworking, Pedoman dan pengaturan mengenai telekomukasi harus mencakup:

(1) Penyediaan peralatan khusus kegiatan teleworking oleh kantor, dimana penggunaan peralatan kantor hanya digunakan untuk keperluan kantor.

(2) Penyediaan peralatan komunikasi yang sesuai, termasuk metode untuk mengamankan akses jarak jauh.

(3) Keamanan fisik perangkat keras.

(4) Penyediaan dukungan dan pemeliharaan perangkat keras dan perangkat lunak (asuransi dan bantuan service)

(5) Prosedur untuk *backup* data.

(6) Audit dan pemantauan keamanan;

(7) Pencabutan wewenang dan hak akses, dan pengembalian peralatan saat kegiatan teleworking dihentikan/sudah waktunya diambil kembali oleh sekolah.

b) Klausul 9 pada Kontrol Akses, kebijakan mengenai hal tersebut harus mempertimbangkan:

(Persyaratan keamanan aplikasi sekolah yang dipakai oleh guru (MySchool, Kafiqu dan EMIS).

(1) Konsistensi antara hak akses dan kebijakan akses pada informasi sistem dan jaringan.

(2) Pengelolaan hak akses yang tepat sesuai bidang dalam sekolah, pada semua jenis koneksi yang disediakan KIIS, dalam hal ini adalah akses Mikrotik.

(3) Pemisahan peran kontrol akses, misalkan permintaan akses, otorisasi akses, administrasi akses kepada kepala labkom selaku administrator.

(4) Persyaratan untuk otorisasi harus resmi dari administrator dan didokumentasikan.

(5) Peninjauan berkala akan hak-hak akses semua guru agar akses informasi sesuai dengan bidangnya.

(6) Pengarsipan catatan semua peristiwa penting terkait dalam penggunaan hak akses (semua log tersimpan).

(7) Tidak di-*share*-nya informasi hak akses administrator kecuali hanya pada bidang yang berwenang.

Proses untuk mengelola ID pengguna harus mencakup:

(a) Menggunakan ID pengguna unik untuk memungkinkan pengguna untuk ditautkan dan bertanggung jawab atas tindakan mereka dan penggunaan ID bersama hanya diizinkan jika diperlukan untuk keperluan bisnis atau operasional dan harus disetujui dan didokumentasikan;

(b) Segera menonaktifkan atau menghapus ID pengguna dari pengguna yang telah meninggalkan organisasi (seperti pada klausul 9.2.6)

(c) Secara berkala mengidentifikasi dan menghapus atau menonaktifkan ID pengguna yang berlebihan (id ganda);

(d) Memastikan bahwa ID pengguna yang berlebihan tidak diberikan kepada pengguna lain.

c) Klausul 12.3 pada Prosedur *Backup*, hal-hal berikut harus dipertimbangkan merencanakan prosedur pencadangan:

(1) Data/informasi harus utuh, tidak parsial;

(2) Tingkat dan frekuensi cadangan harus dijadwalkan teratur;

(3) Cadangan harus disimpan di lokasi khusus, tidak pada lokasi-lokasi umum. Dalam hal ini, KIIS sudah melakukan dengan penempatan server yang jauh dari tempat umum.

(4) Media cadangan (*hdd server*) harus diuji (*chkdisk*) secara berkala untuk memastikan bahwa perangkay penyimpanan tersebut dapat diandalkan untuk penggunaan darurat. Ini harus dilengkapi dengan uji restorasi data. Melakukan *backup* tanpa *overwrite data* yang lama, dalam artian jika ada kegagalan dalam pencadangan, cadangan data yang sebelumnya masih tersedia;

(5) Pada data yang sangat penting, cadangan harus dilindungi dengan cara enkripsi.

d) Klausul 12.6 pada Pengaturan Operasional Perangkat Lunak, panduan berikut harus diikuti dan didokumentasikan untuk menerapkan prosedur yang baik:

(1) Organisasi harus menetapkan peran dan tanggung jawab yang terkait dengan kerentanan *(vulnerability),* termasuk ceklis pemantauan kerentanan, penilaian risiko kerentanan, perbaikan, *log* dokumentasi aset, dan koordinasi tanggung jawab pada bidangnya masing-masing;

(2) Log ceklis evaluasi harus disimpan untuk semua prosedur yang dilakukan;

(3) Proses manajemen kerentanan teknis harus secara teratur dipantau dan dievaluasi untuk memastikan efektivitas dan efisiensinya;

(4) Sistem yang berisiko tinggi harus ditangani terlebih dahulu, dalam hal ini fungsi aplikasi MySchool harus mendapat perhatia lebih mengingat ini adalah aplikasi pusat kegiatan KBM sekolah;

(5) Proses manajemen kerentanan teknis ini harus diselaraskan dengan kegiatan manajemen insiden, untuk mengformulasikan tentang kerentanan data sebelum terjadi insiden;

(6) Menetapkan prosedur antisipasi jika timbul kerentanan risiko dan mengawasinya sehingga dapat membantu menentukan tindakan korektif yang cepat dan tepat.

Aplikasi Pencadangan, aplikasi yang dikembangkan KIIS sudah cukup aman dan multifungsi, sudah sangat terintegrasi dengan baik, namun belum menyentuh mengenai *backup* data. Mengingat data yang banyak memerlukan penyimpanan yang banyak, penulis tetap menganjurkan bahwa aplikasi *backup* yang dipakai adalah aplikasi linux server dan mempunyai fitur *backup* secara berkala.

V. KESIMPULAN

Berdasarkan penguraian pada bab sebelumnya, penulis menyimpulkan penelitian pada Keamanan Sistem Informasi di Kafila International Islamic School ini adalah: penelitian evaluasi keamanan sistem informasi Kafila *International Islamic School* dengan Standar ISO 27002:2013 menggunakan klausul 5 mengenai Kebijakan Keamanan Informasi, klausul 6 mengenai Keamanan Informasi Organisasi, klausul 7 mengenai Keamanan Sumber Daya, klausul 8 mengenai Manajemen Aset, klausul 9 mengenai Kontrol Akses, klausul 11 mengenai Keamanan Fisik dan Lingkungan, klausul 12 mengenai Keamanan Informasi dan klausul 14 mengenai Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan. Pada pengukuran tingkat resiko, semua aset yang diukur mempunyai high risk, artinya hampir semua aset sangat penting dan berpengaruh pada kelangsungan kegiatan organisasi. Namun berbeda dengan setelah dilakukan penelitian, KIIS sudah mempunyai dokumentasi *(log)* yang cukup baik. Hanya ada 3 klausul yang mempunyai nilai rendah yaitu keamanan fisik/lingkungan, keamanan operasi dan Akusisi sistem informasi, pembangunan dan pemeliharaan. Adapun pasal yang paling rendah, adalah:

1) *Pada klausul keamanan fisik/lingkungan,* sangat kurang pada kebijakan pembatasan masuk ruangan, masih terjadi keluar/masuk ruangan penting (seperti ruang labkom dan ruang kontrol) tanpa izin dan belum adanya sanksi pelanggaran jika ada SDM yang melakukan hal tersebut.

2) Pada klausul keamanan operasi, sangat lemah terhadap proteksi data, termasuk di dalamnya belum ada prosedur *backup data* server, prosedur penggunaan aplikasi hingga belum adanya *log* yang rapih dan pengawasan akses secara berkala terhadap aplikasi-aplikasi yang digunakan KIIS.

3) Pada klausul pemeliharaan sistem aplikasi, sangat kurang pada proses testing, belum ada pembuatan panduan penggunaan aplikasi, belum adanya tester aplikasi hingga pada peninjauan kembali aplikasi secara berkala. Perbaikan terjadi jika/hanya ditemukan *bug/error* saja.

Rata-rata penilaian dari semua klausul yang diteliti adalah *managed*, artinya Kafila *International Islamic School* sudah hampir menjalankan dokumentasi keamanan sistem informasi (sebagian dokumentasi terbantu oleh implementasi dokumentasi ISO 9001:2008). Dengan temuan pada sistem manajamen IT KIIS, KIIS dapat membuat SOP-SOP baru yang berhubungan dengan Aset IT dan Aplikasi KIIS, seperti SOP pada pembuatan dan pemakaian aplikasi, pencatatan dan pemeliharaan aset yang lengkap dan teratur, pelatihan-pelatihan keamanan dan aplikasi keamanan hingga

pada sanksi terhadap pelanggaran penggunaan aset IT dan aplikasi untuk tujuan yang tidak semestinya.

Referensi

[1] I. Santosa and D. Kuswanto, "Analisa Manajemen Resiko Keamanan Informasi pada Kantor Pelayanan Pajak Pratama XYZ," vol. 9, no. 2, pp. 108-115, 2016.

[2] H.K. Fitriyadi, "Integrasi teknologi informasi komunikasi dalam pendidikan: potensi manfaat, masyarakat berbasis pengetahuan, pendidikan nilai, strategi implementasi dan pengembangan profesional," vol. 21, no. 3, 2013.

[3] J. Ward and J. Peppard, *Strategic planning for information systems*. John Wiley & Sons, Inc, 2002.

[4] R. Yustiani and R. J.Yunanto, "Peran Marketplace Sebagai Alternatif Bisnis di Era Teknologi Informasi," vol. 6, no. 2, 2017.

[5] M. Pribadi, "Penerapan tata kelola teknologi informasi dengan menggunakan COBIT Framework 4.1 (studi kasus pada RSUD Bari Palembang)," vol. 4, no. 2, pp. 115-124, 2015.

[6] M. Chander, S. K. Jain, and R. Shankar, "Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach," 2013.

[7] F. Mauladani, "Perancangan Sistem Manajemen Keamanan Informasi (Smki) Berdasarkan Sni Iso/Iec 27001: 2013 Dan Sni Iso/Iec 27005: 2013 (Studi Kasus Dptsi-Its)," Institut Teknologi Sepuluh Nopember, 2017.

[8] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," vol. 2, no. 2, pp. 1-8, 2017.

[9] R. Amalyah, D. Hamid, and L. B. Hakim, "Peran stakeholder pariwisata dalam pengembangan Pulau Samalona sebagai destinasi wisata bahari," vol. 37, no. 1, pp. 158-163, 2016.

[10] M. S. Mustaqbal, R. F. Firdaus, and H. Rahmadi, "Pengujian aplikasi menggunakan black box testing boundary value analysis (studi kasus: Aplikasi prediksi kelulusan smnptn)," vol. 1, no. 3, 2015.

[11] K. H. Dewantara, "Identifikasi, Penilaian, dan Mitigasi Risiko Keamanan Informasi Berdasarkan Standar ISO 27001: 2005 dan ISO 27002: 2013 Menggunakan Metode Fmea (Studi Kasus: ISNET)," Institut Teknologi Sepuluh Nopember, 2016.

[12] S. Hariyanto, "Sistem Informasi Manajemen," vol. 9, no. 1, pp. 80-85, 2016.

[13] D. D. Laksana, S. Ismail, and N. A. S.Hendrarini, "Implementasi Honeypot Dengan Modern Honey Network," vol. 3, no. 3, 2017.

[14] E. D. Meutia, "Internet of things–Keamanan dan Privasi," in *Seminar Nasional dan Expo Teknik Elektro*, 2015, vol. 1, no. 1, pp. 85-89.

[15] B. Purnomo, "Metodedan Teknik Pengumpulan Data dalam Penelitian Tindakan Kelas (Classroomaction Research)," vol. 8, no. 1, p. 210251, 2011.