BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1 Identifikasi Klausul ISO 27001

Klausul yang akan digunakan dalam penelitian ini ada 11, yaitu A5 (kebijakan keamanan), A6 (organisasi keamanan informasi), A7 (pengelolaan aset), A8 (keamanan sumber daya manusia), A9 (keamanan fisik dan lingkungan), A10 (pengelolaan operasi dan komunikasi), A11 (pengendalian akses), A12 (akuisisi sistem informasi, pengembangan, dan pemeliharaan), A13 (pengelolaan peristiwa keamanan informasi), A14 (pengelolaan bisnis yang berkelanjutan), dan A15 (pemenuhan).

4.2 Identifikasi Objektif kontrol ISO 27001

Berdasarkan klausul yang ditetapkan, terdapat 39 objektif kontrol yang akan digunakan dalam penelitian ini yang dapat dilihat pada tabel di bawah ini.

Tabel 4.1 Objektif Kontrol ISO 27001

KLAUSUL	OBJEKTIF KONTROL
A5. Kebijakan keamanan	A5.1 Kebijakan keamanan informasi
A6. Organisasi keamanan informasi	A6.1 Organisasi internal
	A6.2 Pihak luar
A7. Pengelolaan aset	A7.1 Tanggung jawab terhadap aset
	A7.2 Klasifikasi informasi
A8. Keamanan sumberdaya manusia	A8.1 Sebelum menjadi karyawan
	A8.2 Selama menjadi karyawan
	A8.3 Penghentian atau mutasi karyawan
A9. Keamanan fisik dan lingkungan	A9.1 Area yang aman
	A9.2 Keamanan peralatan
A10. Pengelolaan operasi dan komunikasi	A10.1 Tanggung jawab dan prosedur operasional
	A10.2 Pengelolaan penyerahan layanan pihak ketiga
	A10.3 Sistem perencanaan dan penerimaan
	A10.4 Perlindungan melawan kode *malicious* dan *mobile*
	A10.5 *Back up*

	A10.6 Pengelolaan keamanan jaringan
	A10.7 Penanganan media
	A10.8 Pertukaran informasi
	A10.9 Pelayanan perniagaan elektronik
	A10.10 Pengawasan
A11. Pengendalian akses	A11.1 Persyaratan bisnis untuk pengendalian akses
	A11.2 Manajemen akses pengguna
	A11.3 Tanggungjawab pengguna
	A11.4 Pengendalian akses jaringan
	A11.5 Pengendalian akses sistem operasi
	A11.6 Pengendalian aplikasi dan sistem informasi
	A11.7 *Mobile computing* dan kerja jarak jauh (*teleworking*)
A12. Akuisisi sistem informasi, pengembangan dan pemeliharaan	A12.1 Kebutuhan keamanan sistem informasi
	A12.2 Pemprosesan yang benar di aplikasi
	A12.3 Pengendalian kriptograpi
	A12.4 Keamanan file sistem
	A12.5 Keamanan di dalam proses pendukung dan pengembangan
	A12.6 Pengelolaan teknik penyerangan
A13. Pengelolaan peristiwa keamanan informasi	A13.1 Laporan kelemahan dan peristiwa keamanan informasi
	A13.2 Pengelolaan perbaikan dan peristiwa keamanan informasi
A14. Pengelolaan bisnis yang berkelanjutan	A14.1 Aspek keamanan informasi untuk pengelolaan bisnis yang berkelanjutan
A15. Pemenuhan	A15.1 Pemenuhan kebutuhan yang legal
	A15.2 Pemenuhan kebijakan dan standar keamanan dan pemenuhan teknik
	A15.3 Pertimbangan audit sistem informasi

4.3 Identifikasi Kontrol Keamanan ISO 27001

Setelah ditentukan objektif kontrol, peneliti menentukan kontrol keamanan yang akan digunakan dalam penelitian ini yang dapat dilihat pada tabel berikut.

Tabel 4.2 Kontrol Keamanan ISO 27001

	KONTROL KEAMANAN

OBJEKTIF KONTROL	
A5.1 Kebijakan keamanan informasi	dokumen kebijakan keamanan informasi
	pengulasan kebijakan keamanan informasi
A6.1 Organisasi internal	komitmen manajemen terhadap kontrol keamanan informasi
	kendali koordinasi keamanan informasi
	alokasi kendali merespon keamanan informasi
	proses otorisasi untuk kendali fasilitas pemproses informasi
	persetujuan tentang kerahasiaan
	hubungan dengan otorisasi
	hubungan dengan group yang memiliki keterkaitan khusus
	keamanan informasi terhadap ulasan mandiri
A6.2 Pihak luar	identifikasi hubungan resiko pihak luar
	penunjukan keamanan ketika berhadapan dengan customer
	penunjukan keamanan di dalam persetujuan pihak ketiga
A7.1 Tanggung jawab terhadap aset	inventaris aset
	kepemilikan aset
	penggunaan yang cocok terhadap aset
A7.2 Klasifikasi informasi	petunjuk klasifikasi
	penanganan dan pelabelan informasi
A8.1 Sebelum menjadi karyawan	peraturan dan pertanggungjawaban
	Penyaringan
	terminologi dan kondisi karyawan
A8.2 Selama menjadi karyawan	tanggungjawab manajemen
	pelatihan, pendidikan dan kesadaran keamanan informasi
	proses pendisiplinan
A8.3 Penghentian atau mutasi karyawan	tanggungjawab penghentian
	pengembalian aset
	pemindahan hak akses
A9.1 Area yang aman	garis pertahanan keamanan fisik
	kendali masukan fisik
	fasilitas, ruangan, dan kantor yang aman
	perlindungan terhadap ancamanan lingkungan luar
	pekerjaan di area keamanan
	area akses umum, penyerahan, dan pemuatan
A9.2 Keamanan peralatan	perlindungan dan peletakan peralatan
	keperluan pendukung
	keamanan pemasangan kabel
	perawatan peralatan
	Keamanan dalam pengambilan alat-alat asumsi
	jaminan pembuangan atau penggunaan kembali peralatan

	pemusnahan properti
A10.1 Tanggung jawab dan prosedur operasional	prosedur operasi yang didokumentasikan
	pengelolaan perubahaan
	pemisahan tugas
	pemisahan fasilitas operasional, tes, dan pengembangan
A10.2 Pengelolaan penyerahan layanan pihak ketiga	penyerahan layanan
	pengawasan dan pengulasan layanan pihak ketiga
	mengelola perubahan layanan pihak ketiga
A10.3 Sistem perencanaan dan penerimaan	pengelolaan kapasitas
	sistem penerimaan
A10.4 Perlindungan melawan kode malicious dan mobile	kontrol melawan kode malicious
	kontrol melawan kode mobile
A10.5 Back up	back up informasi
A10.6 Pengelolaan keamanan jaringan	kendali jaringan
	keamanan pelayanan jaringan
A10.7 Penanganan media	pengelolaan pemindahan media
	pembuangan media
	prosedur penanganan informasi
	keamanan dokumentasi sistem
A10.8 Pertukaran informasi	prosedur dan kebijakan pertukaran informasi
	persetujuan pertukaran
	media fisik di perjalanan
	pesan elektronik
	sistem informasi bisnis
A10.9 Pelayanan perniagaan elektronik	perniagaan elektronik
	transaksi online
	informasi tersedia di depan umum
A10.10 Pengawasan	membukukan audit
	penggunaan sistem pengawasan
	perlindungan log information
	log operator dan administrator
	membukukan kesalahan
	sinkronisasi jam
A11.1 Persyaratan bisnis untuk pengendalian	kebijakan kendali akses

akses	
A11.2 Manajemen akses pengguna	registrasi pengguna
	pengelolaan hak
	pengelolaan sandi pengguna
	pengulasan kebenaran akses pengguna
A11.3 Tanggungjawab pengguna	penggunaan sandi
	peralatan pengguna tidak dapat dihadirkan
	kebijakan tabir dan bagian yang transparansi
A11.4 Pengendalian akses jaringan	kebijakan pengguna layanan jaringan
	pembuktian keaslian pengguna untuk koneksi eksternal
	identifikasi peralatan jaringan
	konfigurasi dan diagnosa perlindungan port
	pemisahan jaringan
	kendali koneksi jaringan
	kendali routing jaringan
A11.5 Pengendalian akses sistem operasi	prosedur masuk dalam keamanan
	pengesahan dan identifikasi pengguna
	sistem pengelolaan kata sandi
	menggunakan fungsi sistem
	sesi waktu habis
	pembatasan waktu koneksi
A11.6 Pengendalian aplikasi dan sistem informasi	pembatasan akses informasi
	pengisolasian sistem yang sensitif
A11.7 Mobile computing dan kerja jarak jauh	komunikasi dan mobile computing
	Teleworking
A12.1 Kebutuhan keamanan sistem informasi	spesifikasi dan analisis kebutuhan keamanan
A12.2 Pemprosesan yang benar di aplikasi	validasi data masukan
	kendali pemprosesan internal
	integritas pesan
	validasi data keluaran
A12.3 Pengendalian kriptograpi	kebijakan menggunakan kendali kriptograpi
	pengelolaan kunci
A12.4 Keamanan file sistem	kendali perangkat lunak operasional
	perlindungan data pengujian sistem
	kendali akses untuk kode sumber program
	prosedur kendali perubahan

A12.5 Keamanan di dalam proses pendukung dan pengembangan	pengulasan teknik aplikasi setelah perubahan sistem operasi
	membatasi perubahan paket perangkat lunak
	kebocoran informasi
	sumberdaya pengembangan perangkat lunak
A12.6 Pengelolaan teknik penyerangan	kendali teknik penyerangan
A13.1 Laporan kelemahan dan peristiwa keamanan informasi	laporan peristiwa keamanan informasi
	laporan kelemahan keamanan
A13.2 Pengelolaan perbaikan dan peristiwa keamanan informasi	prosedur dan tanggungjawab
	belajar dari peristiwa keamanan informasi
	kumpulan bukti
A14.1 Aspek keamanan informasi untuk pengelolaan bisnis yang berkelanjutan	keamanan informasi mencakup proses pengelolaan bisnis yang berkelanjutan
	penaksiran resiko dan bisnis yang berkelanjutan
	keamanan informasi meliputi rencana pengembangan dan implementasi berkelanjutan
	kerangka rencana bisnis berkelanjutan
	menaksir, merawat, dan menguji rencana bisnis berkelanjutan
A15.1 Pemenuhan kebutuhan yang legal	identifikasi perundang-undangan yang dipergunakan
	kekayaan intelektual yang benar
	perlindungan catatan organisasi
	perlindungan dan kerahasian data informasi personal
	mencegah penyalahgunaan fasilitas pemprosesan informasi
	peraturan kendali kriptograpi
A15.2 Pemenuhan kebijakan dan standar keamanan dan pemenuhan teknik	pemenuhan standar dan kebijakan keamanan
	memeriksa pemenuhan teknis
A15.3 Pertimbangan audit sistem informasi	kendali audit sistem informasi
	perlindungan alat audit informasi

4.4 Uji Validitas dan Reliabilitas

Pada sub bab ini akan diuji validitas kuesioner yang digunakan untuk mengukur sah atau tidaknya atau ketepatan alat ukur penelitian dengan isi sebenarnya yang diukur. Uji validitas dapat dihitung dengan bantuan IBM SPSS Statistic versi 24 menggunakan persamaan sebagai berikut.

$$r_{yx} = \frac{n\sum XY - (\sum X)(\sum Y)}{\sqrt{\{n\sum X^2 - (\sum X)^2\}\{n\sum Y^2 - (\sum Y)^2\}}}$$

Keterangan :

r_{yx} = koefisien korelasi *Pearson Product Moment*

X = skor item

Y = skor item total

N = jumlah responden

Data kuisioner yang diperoleh dari responden telah diuji validitasnya menggunakan IBM SPSS Statistic versi 24. Kriteria pengambilan keputusan adalah sebagai berikut.

Bila $r_{hitung} > r_{tabel}$ maka instrumen valid. Bila $r_{hitung} < r_{tabel}$ maka instrumen tidak valid. Uji validitas pada penelitian ini dilakukan tiap item pernyataan pada kerangka kerja ISO 27001. Hasil uji validitas untuk kondisi saat ini *(performance)* dapat dilihat pada tabel 4.3.

Tabel 4.3 Hasil Uji Validitas Data Responden

NO	KONTROL KEAMANAN	r_{xy}	r_{tabel}	KETERANGAN
1	A5.1.1	1,000	0,8054	Valid
2	A5.1.2	1,000	0,8054	Valid
3	A6.1.1	0,996	0,8054	Valid
4	A6.1.2	0,996	0,8054	Valid
5	A6.1.3	0,996	0,8054	Valid
6	A6.1.4	0,891	0,8054	Valid
7	A6.1.5	0,996	0,8054	Valid
8	A6.1.6	0,996	0,8054	Valid
9	A6.1.7	0,891	0,8054	Valid
10	A6.1.8	0,996	0,8054	Valid
11	A6.2.1	0,980	0,8054	Valid
12	A6.2.2	0,976	0,8054	Valid
13	A6.2.3	0,980	0,8054	Valid
14	A7.1.1	0,975	0,8054	Valid
15	A7.1.2	0,983	0,8054	Valid
16	A7.1.3	0,983	0,8054	Valid
17	A7.2.1	1,000	0,8054	Valid
18	A7.2.2	1,000	0,8054	Valid
19	A8.1.1	1,000	0,8054	Valid
20	A8.1.2	1,000	0,8054	Valid
21	A8.1.3	1,000	0,8054	Valid
22	A8.2.1	1,000	0,8054	Valid
23	A8.2.2	1,000	0,8054	Valid
24	A8.2.3	1,000	0,8054	Valid
25	A8.3.1	1,000	0,8054	Valid
26	A8.3.2	1,000	0,8054	Valid
27	A8.3.3	1,000	0,8054	Valid
28	A9.1.1	1,000	0,8054	Valid
29	A9.1.2	1,000	0,8054	Valid
30	A9.1.3	1,000	0,8054	Valid
31	A9.1.4	1,000	0,8054	Valid
32	A9.1.5	1,000	0,8054	Valid
33	A9.1.6	1,000	0,8054	Valid
34	A9.2.1	1,000	0,8054	Valid
35	A9.2.2	1,000	0,8054	Valid
36	A9.2.3	1,000	0,8054	Valid
37	A9.2.4	1,000	0,8054	Valid
38	A9.2.5	1,000	0,8054	Valid
39	A9.2.6	1,000	0,8054	Valid
40	A9.2.7	1,000	0,8054	Valid
41	A10.1.1	0,970	0,8054	Valid
42	A10.1.2	0,970	0,8054	Valid

NO	KONTROL KEAMANAN	r_{xy}	r_{tabel}	KETERANGAN
43	A10.1.3	0,970	0,8054	Valid
44	A10.1.4	0,922	0,8054	Valid
45	A10.2.1	0,976	0,8054	Valid
46	A10.2.2	0,976	0,8054	Valid
47	A10.2.3	0,958	0,8054	Valid
48	A10.3.1	1,000	0,8054	Valid
49	A10.3.2	1,000	0,8054	Valid
50	A10.4.1	1,000	0,8054	Valid
51	A10.4.2	1,000	0,8054	Valid
52	A10.5.1	1,000	0,8054	Valid
53	A10.6.1	0,919	0,8054	Valid
54	A10.6.2	0,919	0,8054	Valid
55	A10.7.1	0,975	0,8054	Valid
56	A10.7.2	0,975	0,8054	Valid
57	A10.7.3	0,975	0,8054	Valid
58	A10.7.4	0,907	0,8054	Valid
59	A10.8.1	1,000	0,8054	Valid
60	A10.8.2	1,000	0,8054	Valid
61	A10.8.3	1,000	0,8054	Valid
62	A10.8.4	1,000	0,8054	Valid
63	A10.8.5	1,000	0,8054	Valid
64	A10.9.1	1,000	0,8054	Valid
65	A10.9.2	1,000	0,8054	Valid
66	A10.9.3	1,000	0,8054	Valid
67	A10.10.1	1,000	0,8054	Valid
68	A10.10.2	1,000	0,8054	Valid
69	A10.10.3	1,000	0,8054	Valid
70	A10.10.4	1,000	0,8054	Valid
71	A10.10.5	1,000	0,8054	Valid
72	A10.10.6	0,919	0,8054	Valid
73	A11.1.1	1,000	0,8054	Valid
74	A11.2.1	0,986	0,8054	Valid
75	A11.2.2	0,986	0,8054	Valid
76	A11.2.3	0,986	0,8054	Valid
77	A11.2.4	0,943	0,8054	Valid
78	A11.3.1	0,983	0,8054	Valid
79	A11.3.2	0,983	0,8054	Valid
80	A11.3.3	0,975	0,8054	Valid
81	A11.4.1	1,000	0,8054	Valid
82	A11.4.2	1,000	0,8054	Valid
83	A11.4.3	1,000	0,8054	Valid
84	A11.4.4	1,000	0,8054	Valid

NO	KONTROL KEAMANAN	r_{xy}	r_{tabel}	KETERANGAN
85	A11.4.5	1,000	0,8054	Valid
86	A11.4.6	1,000	0,8054	Valid
87	A11.4.7	1,000	0,8054	Valid
88	A11.5.1	0,994	0,8054	Valid
89	A11.5.2	0,994	0,8054	Valid
90	A11.5.3	0,953	0,8054	Valid
91	A11.5.4	0,994	0,8054	Valid
92	A11.5.5	0,994	0,8054	Valid
93	A11.5.6	0,994	0,8054	Valid
94	A11.6.1	1,000	0,8054	Valid
95	A11.6.2	1,000	0,8054	Valid
96	A11.7.1	1,000	0,8054	Valid
97	A11.7.2	1,000	0,8054	Valid
98	A12.1.1	1,000	0,8054	Valid
99	A12.2.1	0,990	0,8054	Valid
100	A12.2.2	0,990	0,8054	Valid
101	A12.2.3	0,990	0,8054	Valid
102	A12.2.4	0,965	0,8054	Valid
103	A12.3.1	1,000	0,8054	Valid
104	A12.3.2	1,000	0,8054	Valid
105	A12.4.1	1,000	0,8054	Valid
106	A12.4.2	1,000	0,8054	Valid
107	A12.4.3	1,000	0,8054	Valid
108	A12.5.1	0,993	0,8054	Valid
109	A12.5.2	0,993	0,8054	Valid
110	A12.5.3	0,958	0,8054	Valid
111	A12.5.4	0,993	0,8054	Valid
112	A12.5.5	0,993	0,8054	Valid
113	A12.6.1	1,000	0,8054	Valid
114	A13.1.1	1,000	0,8054	Valid
115	A13.1.2	1,000	0,8054	Valid
116	A13.2.1	0,968	0,8054	Valid
117	A13.2.2	0,968	0,8054	Valid
118	A13.2.3	0,968	0,8054	Valid
119	A14.1.1	1,000	0,8054	Valid
120	A14.1.2	0.919	0,8054	Valid
121	A14.1.3	0.919	0,8054	Valid
122	A14.1.4	1,000	0,8054	Valid
123	A14.1.5	1,000	0,8054	Valid
124	A15.1.1	0,994	0,8054	Valid
125	A15.1.2	0,994	0,8054	Valid
126	A15.1.3	0,895	0,8054	Valid

NO	KONTROL KEAMANAN	r_{xy}	r_{tabel}	KETERANGAN
127	A15.1.4	0,895	0,8054	Valid
128	A15.1.5	0,994	0,8054	Valid
129	A15.1.6	0,994	0,8054	Valid
130	A15.2.1	1,000	0,8054	Valid
131	A15.2.2	1,000	0,8054	Valid
132	A15.3.1	0,968	0,8054	Valid
133	A15.3.2	0,988	0,8054	Valid

Berdasarkan hasil uji validitas masing-masing instrumen, hasil yang didapatkan yaitu nilai r $_{hitung}$> r $_{tabe}$l dimana nilai r $_{hitung}$, yaitu 0,8054 (berdasarkan tabel r $_{tabe}$l terlampir). Dengan demikian item pernyataan kuesioner yang valid berjumlah 133.

Kemudian dilakukan uji reliabilitas statistik pada data responden menggunakan metode alpha cronbach's. Pada tabel 4.4 ditampilkan nilai *cronbach's alpha* untuk masing-masing *item* instrumen.

Tabel 4.4 *Reliability Statistics*

OBJECTIVE CONTROL	N	N of items	CRONBACH'S ALPHA
A5.1.1	5	2	1,000
A5.1.2			
A6.1.1	5	8	0,982
A6.1.2			
A6.1.3			
A6.1.4			
A6.1.5			
A6.1.6			
A6.1.7			

OBJECTIVE CONTROL	N	N of items	CRONBACH'S ALPHA
A6.1.8			
A6.2.1	5	3	0,929
A6.2.2			
A6.2.3			
A7.1.1	5	3	0,947
A7.1.2			
A7.1.3			
A7.2.1	5	2	0,889
A7.2.2			
A8.1.1	5	3	1,000
A8.1.2			
A8.1.3			
A8.2.1	5	3	1,000
A8.2.2			
A8.2.3			
A8.3.1	5	3	0,938
A8.3.2			
A8.3.3			
A9.1.1	5	6	1,000
A9.1.2			
A9.1.3			
A9.1.4			
A9.1.5			
A9.1.6			
A9.2.1	5	7	1,000

OBJECTIVE CONTROL	N	N of items	CRONBACH'S ALPHA
A9.2.2			
A9.2.3			
A9.2.4			
A9.2.5			
A9.2.6			
A9.2.7			
A10.1.1	5	4	0,930
A10.1.2			
A10.1.3			
A10.1.4			
A10.2.1	5	3	0,943
A10.2.2			
A10.2.3			
A10.3.1	5	2	1,000
A10.3.2			
A10.4.1	5	2	1,000
A10.4.2			
A10.5.1	5	1	.
A10.6.1	5	2	1,000
A10.6.2			
A10.7.1	5	4	0,947
A10.7.2			
A10.7.3			
A10.7.4			
A10.8.1	5	5	1,000

OBJECTIVE CONTROL	N	N of items	CRONBACH'S ALPHA
A10.8.2			
A10.8.3			
A10.8.4			
A10.8.5			
A10.9.1	5	3	1,000
A10.9.2			
A10.9.3			
A10.10.1	5	6	0,984
A10.10.2			
A10.10.3			
A10.10.4			
A10.10.5			
A10.10.6			
A11.1.1	5	1	.
A11.2.1	5	4	0,966
A11.2.2			
A11.2.3			
A11.2.4			
A11.3.1	5	3	0,947
A11.3.2			
A11.3.3			
A11.4.1	5	7	0,984
A11.4.2			
A11.4.3			
A11.4.4			

OBJECTIVE CONTROL	N	N of items	CRONBACH'S ALPHA
A11.4.5			
A11.4.6			
A11.4.7			
A11.5.1	5	6	0,978
A11.5.2			
A11.5.3			
A11.5.4			
A11.5.5			
A11.5.6			
A11.6.1	5	2	1,000
A11.6.2			
A11.7.1	5	2	1,000
A11.7.2			
A12.1.1	5	1	.
A12.2.1	5	4	0,968
A12.2.2			
A12.2.3			
A12.2.4			
A12.3.1	5	2	1,000
A12.3.2			
A12.4.1	5	3	0,938
A12.4.2			
A12.4.3			
A12.5.1	5	5	0,978
A12.5.2			

OBJECTIVE CONTROL	N	N of items	CRONBACH'S ALPHA
A12.5.3			
A12.5.4			
A12.5.5			
A12.6.1	5	1	.
A13.1.1	5	2	0,889
A13.1.2			
A13.2.1	5	3	0,900
A13.2.2			
A13.2.3			
A14.1.1	5	5	0,961
A14.1.2			
A14.1.3			
A14.1.4			
A14.1.5			
A15.1.1	5	6	0,969
A15.1.2			
A15.1.3			
A15.1.4			
A15.1.5			
A15.1.6			
A15.2.1	5	2	1,000
A15.2.2			
A15.3.1	5	2	0,900
A15.3.2			

Dari nilai cronbach alpha *if item deleted* di atas memiliki nilai lebih besar dari 0,6 maka dapat disimpulkan bahwa instrumen reliabel atau konsisten.

4.5 Analisa Kesenjangan

Berdasarkan hasil pengukuran tingkat kematangan keamanan informasi saat ini yang kemudian dibandingkan dengan harapan pihak manajemen sekolah, diperoleh tingkat kesenjangan sebagai berikut.

Tabel 4.5 Kesenjangan (*gap*)

OBJEKTIF KONTROL	CURRENT MATURITY LEVEL	EXPECT MATURITY LEVEL	GAP
A5.1	2,40	4	1,60
A6.1	2,65	4	1,35
A6.2	2,73	4	1,27
A7.1	2,47	4	1,53
A7.2	2,30	4	1,70
A8.1	2,40	4	1,60
A8.2	2,40	4	1,60
A8.3	2,53	4	1,47
A9.1	2,40	4	1,60
A9.2	2,40	4	1,60
A10.1	2,90	4	1,10
A10.2	2,67	4	1,33
A10.3	2,80	4	1,20
A10.4	2,40	4	1,60
A10.5	2,60	4	1,40
A10.6	2,60	4	1,40
A10.7	2,85	4	1,15
A10.8	2,60	4	1,40
A10.9	2,80	4	1,20
A10.10	2,43	4	1,57
A11.1	2,60	4	1,40
A11.2	2,65	4	1,35
A11.3	2,47	4	1,53
A11.4	2,46	4	1,54
A11.5	2,67	4	1,33
A11.6	2,40	4	1,60
A11.7	2,20	4	1,80
A12.1	2,20	4	1,80
A12.2	2,45	4	1,55

OBJEKTIF KONTROL	CURRENT MATURITY LEVEL	EXPECT MATURITY LEVEL	GAP
A12.3	2,20	4	1,80
A12.4	2,27	4	1,73
A12.5	2,44	4	1,56
A12.6	2,60	4	1,40
A13.1	2,30	4	1,70
A13.2	2,33	4	1,67
A14.1	2,48	4	1,52
A15.1	2,67	4	1,33
A15.2	2,80	4	1,20
A15.3	2,50	4	1,50

Berdasarkan data yang ada, dapat dianalisa hasil temuan masalah pada keamanan informasi sekolah adalah sebagai berikut.

1. A5 Kebijakan Keamanan
   Dari proses perhitungan diperoleh nilai rata-rata pada klausul kebijakan keamanan dengan nilai 2,40 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 2 (*repeatable*), yang berarti institusi telah memiliki pola yang berulang kali dilakukan dalam manajemen aktivitas terkait dengan tata kelola teknologi, namun keberadaanya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidak konsistenan. Pada klausul kebijakan keamanan terdapat *gap* 1,60 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen, sehingga butuh penetapan kebijakan keamanan informasi institusi secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkanya.
2. A6 Organisasi Keamanan Informasi
   Dari proses perhitungan diperoleh nilai rata-rata pada klausul organisasi keamanan informasi dengan nilai 2,67 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*), yang berarti institusi telah memiliki prosedur baku formal dan tertulis yang telah disosialisasikan ke segenap jajaran dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul organisasi keamanan informasi terdapat *gap* 1,31 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak

manajemen oleh karena itu, institusi harus memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggung jawab mengelola keamanan informasi dan menjaga kepatuhanya.

3. A7 Pengelolaan Aset

   Dari proses perhitungan diperoleh nilai rata-rata pada klausul pengelolaan aset dengan nilai 2,40 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 2 (*repeatable*), yang berarti institusi telah memiliki pola yang berulang kali dilakukan dalam manajemen aktivitas terkait dengan tata kelola teknologi, namun keberadaanya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidak konsistenan. Pada klausul pengelolaan aset terdapat *gap 1,62* dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen, maka perlu diberlakukannya pengklasifikasian data yang dapat diakses oleh *user* sistem informasi.

4. A8 Keamanan Sumber Daya Manusia

   Pada proses perhitungan diperoleh nilai rata-rata pada klausul keamanan sumber daya manusia dengan nilai 2,44 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 2 (*repeatable*), yang berarti institusi telah memiliki pola yang berulang kali dilakukan dalam manajemen aktivitas terkait dengan tata kelola teknologi, namun keberadaanya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidak konsistenan. Pada klausul keamanan sumber daya manusia terdapat *gap* 1,56 dari perbandingan tingkat kematangan saat ini dengan harapan pihak manajemen, oleh karena itu dibutuhkan isi kontrak kerja pegawai membahas tentang tangungjawab terhadap keamanan informasi.

5. A9 Keamanan Fisik dan Lingkungan

   Pada proses perhitungan diperoleh nilai rata-rata pada klausul keamanan fisik dan lingkungan dengan nilai 2,40 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 2 (*repeatable*), yang berarti institusi telah memiliki pola yang berulang kali dilakukan dalam manajemen aktivitas terkait dengan tata kelola teknologi, namun keberadaanya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidak konsistenan. Pada klausul keamanan fisik dan lingkungan terdapat *gap* 1,60 dari perbandingan tingkat

kematangan saat ini dengan yang diharapkan oleh pihak manajemen, oleh karena itu institusi perlu adanya tempat khusus untuk server informasi.

6. A10 Pengelolaan Operasi dan Komunikasi

   Pada proses perhitungan diperoleh nilai rata-rata pada klausul pengelolaan operasi dan komunikasi dengan nilai 2,66 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*), yang berarti bahwa instansi telah memiliki prosedur baku formal dan tertulis yang telah di sosialisasikan ke segenap jajaran dan karyawan tentang kegiatan monitoring, evaluasi, dan penilaian pengelolaan operasi dan komunikasi yang ada di instansi untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul pengelolaan operasi dan komunikasi terdapat *gap* 1,34 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen, maka perlu diberlakukannya kendali pendeteksian, pencegahan dan pemulihan sistem informasi dapat melawan kode *malicious*.

7. A11 Pengendalian Akses

   Pada proses perhitungan diperoleh nilai rata-rata pada klausul pengendalian akses dengan nilai 2,52 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*), yang berarti bahwa instansi telah memiliki prosedur baku formal dan tertulis yang telah disosialisasikan ke segenap jajaran dan karyawan tentang kegiatan monitoring, evaluasi, dan penilaian pengendalian akses sistem informasi yang ada di instansi untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul pengendalian akses terdapat *gap* 1,51 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen, maka dibutuhkan proses *mobile computing* yang dapat membantu meningkatkan kinerja sistem informasi.

8. A12 Akuisisi Sistem Informasi, Pengembangan, dan Pemeliharaan

   Pada proses perhitungan diperoleh nilai rata-rata pada klausul akuisisi sistem informasi, pengembangan, dan pemeliharaan dengan nilai 2,38 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 2 (*repeatable*), yang berarti institusi telah memiliki pola yang berulang kali dilakukan dalam manajemen aktivitas terkait dengan tata kelola teknologi, namun keberadaanya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidak

konsistenan. Pada klausul akuisisi sistem informasi, pengembangan, dan pemeliharaan terdapat *gap* 1,64 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen, oleh karena itu kebutuhan bisnis pada sistem informasi yang baru harus memberikan kendali keamanan yang lebih baik.

9. A13 Pengelolaan Peristiwa Keamanan Informasi
   Pada proses perhitungan diperoleh nilai rata-rata pada klausul pengelolaan peristiwa keamanan informasi dengan nilai 2,32 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 2 (*repeatable*), yang berarti institusi telah memiliki pola yang berulang kali dilakukan dalam manajemen aktivitas terkait dengan tata kelola teknologi, namun keberadaanya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidak konsistenan. Pada klausul pengelolaan peristiwa keamanan informasi terdapat *gap* 1,68 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen, oleh karena itu perlu adanya pelaporan kelemahan keamanan sistem informasi.
10. A14 Pengelolaan Bisnis yang Berkelanjutan
    Pada proses perhitungan diperoleh nilai rata-rata pada klausul pengelolaan bisnis yang berkelanjutan dengan nilai 2,48 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 2 (*repeatable*), yang berarti institusi telah memiliki pola yang berulang kali dilakukan dalam manajemen aktivitas terkait dengan tata kelola teknologi, namun keberadaanya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidak konsistenan. Pada klausul pengelolaan bisnis yang berkelanjutan terdapat *gap* 1,52 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen, oleh karena itu perlu adanya pengelolaan kebutuhan keamanan informasi untuk dikembangkan.
11. A15 Pemenuhan
    Pada proses perhitungan diperoleh nilai rata-rata pada klausul pemenuhan dengan nilai 2,66 yang masuk ke dalam skala pengukuran tingkat kematangan pada level 3 (*define*), yang berarti bahwa instansi telah memiliki prosedur baku formal dan tertulis yang telah disosialisasikan ke segenap jajaran dan karyawan tentang kegiatan monitoring, evaluasi, dan penilaian yang ada

diinstansi untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. Pada klausul pemenuhan terdapat *gap* 1,34 dari perbandingan tingkat kematangan saat ini dengan yang diharapkan oleh pihak manajemen, oleh karena itu perlu adanya aktivitas audit yang melibatkan pengecekan sistem informasi untuk meminimalkan resiko gangguan pada proses bisnis.