BAB II
LANDASAN TEORI

2.1 Tinjauan Organisasi

Tinjauan organisasi berisi penjelasan tentang sejarah, visi, misi, tujuan, struktur organisasi, serta tugas pokok dan fungsi institusi.

2.1.1 Sejarah institusi

SMK Negeri 1 Pugung merupakan salah satu bentuk satuan pendidikan formal yang menyelenggarakan pendidikan kejuruan pada jenjang pendidikan menengah atas yang berdiri pada tanggal 11 Desember 2003 dengan SK pendirian sekolah nomor 402/8544/20/2003. SMK Negeri 1 Pugung dibangun di atas tanah seluas 10.000 m^2.

2.1.2 Visi institusi

Visi SMKN 1 Pugung, yaitu bermutu, unggul merata, terampil, berkarakter, dan berdaya saing dalam kebekerjaan.

2.1.3 Misi institusi

Misi SMKN 1 Pugung, yaitu :

1. Meningkatkan kualitas manajemen sekolah dalam menumbuhkan semangat keunggulan.
2. Meningkatkan kualitas kompetensi guru dan pegawai.
3. Meningkatkan kualitas KBM dalam mencapai kompetensi siswa.
4. Meningkatkan kuantitas dan kualitas sarana dan prasarana pendidikan dalam mendukung penguasaan iptek.
5. Meningkatkan kemitraan dengan dunia usaha/dunia industri.

2.2 Audit

Audit berasal dari bahasa latin "*audire*" yang berarti mendengar atau *to hear,* yaitu pada zaman dahulu apabila seorang pemilik organisasi usaha merasa ada suatu kesalahan atau penyalahgunaan, maka ia mendengarkan kesaksian orang tertentu (Gondodiyoto, 2007).

2.3 Sistem

Menurut Al Fatta (2007), sistem merupakan sekumpulan objek-objek yang saling berelasi dan berinteraksi serta hubungan antar objek yang dilihat sebagai satu kesatuan yang dirancang untuk mencapai satu tujuan. Sistem mempunyai karakteristik sebagai berikut (Mulyanto, 2009) :

1. Mempunyai komponen sistem (*components system*)

   Suatu sistem tidak berada dalam lingkungan yang kosong, tetapi sebuah sistem berada dan berfungsi di dalam lingkungan yang berisi sistem lainnya. Suatu sistem terdiri dari sejumlah komponen yang saling berinteraksi, bekerja sama membentuk satu kesatuan. Apabila suatu sistem merupakan salah satu dari komponen sistem lain yang lebih besar, maka akan disebut dengan subsistem, sedangkan sistem yang lebih besar tersebut adalah lingkungannya.
2. Mempunyai batasan sistem (*boundary*)

   Batas sistem merupakan pembatas atau pemisah antara suatu sistem dengan sistem yang lainnya atau dengan lingkungan luarnya.
3. Mempunyai lingkungan (*environment*)

   Lingkungan luar adalah apa pun di luar batas dari sistem yang dapat mempengaruhi operasi sistem, baik pengaruh yang menguntungkan ataupun yang merugikan. Pengaruh yang menguntungkan ini tentunya harus dijaga sehingga akan mendukung kelangsungan operasi sebuah sistem. Sedangkan lingkungan yang merugikan harus ditahan dan dikendalikan agar tidak mengganggu kelangsungan sebuah sistem.
4. Mempunyai penghubung (*interface*) antar komponen

   Penghubung (*interface*) merupakan media penghubung antara satu subsistem dengan subsistem yang lainnya. Penghubung inilah yang akan menjadi media yang digunakan data dari masukan (*input*) hingga keluaran (*output*). Dengan

adanya penghubung, suatu subsistem dapat berinteraksi dan berintegrasi dengan subsistem yang lain membentuk satu kesatuan.

5. Mempunyai masukan (*input*)

   Masukan atau *input* merupakan energi yang dimasukan ke dalam sistem. Masukan dapat berupa masukan perawatan (*maintenance input*), yaitu bahan yang dimasukkan agar sistem tersebut dapat beroperasi dan masukan sinyal (*signal input*), yaitu masukan yang diproses untuk mendapatkan keluaran.

6. Mempunyai pengolahan (*processing*)

   Pengolahan (*process*) merupakan bagian yang melakukan perubahan dari masukan untuk menjadi keluaran yang diinginkan.

7. Mempunyai sasaran (*objective*) dan tujuan

   Suatu sistem pasti memiliki sasaran (*objective*) atau tujuan *(goal*). Apabila sistem tidak mempunyai sasaran, maka operasi sistem tidak akan ada gunanya. Tujuan inilah yang mengarahkan suatu sistem. Tanpa adanya tujuan, sistem menajdi tidak terarah dan terkendali.

8. Mempunyai keluaran (*output*)

   Keluaran (*output*) merupakan hasil dari pemrosesan. Keluaran dapat berupa informasi sebagai masukan pada sistem lain atau hanya sebagai sisa pembuangan.

9. Mempunyai umpan balik (*feed back*)

   Umpan balik diperlukan oleh bagian kendali (*control*) sistem untuk mengecek terjadinya penyimpangan proses dalam sistem dan mengembalikannya ke dalam kondisi normal.

system is a set of interrelated components, with a clearly defined boundary, working together to achieve a common set of objectives by accepting inputs and producing outputs in an organized transformation process. According to Hardcastle [4] a system can be defined as a collection of components that work together towards a common goal. The objective of a system is to receive inputs and transform these into outputs (Yaser, 2014). *Management information systems*

are formal systems for presenting management with timely and suitable information necessary for decision making (Al-Nakib, 2015).

2.4 Keamanan Informasi

Keamanan informasi saat ini menjadi hal yang sangat penting, terutamam terhadap organisasi yang menggunakan teknologi Informasi (TI) sebagai pendukung proses bisnisnya. Penggunaan TI bertujuan untuk meningkatkan kualitas layanan yang diberikan terhadap para *stakeholder*. Keamanan informasi merupakan penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi resiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (Riyanarto, 2009). Pengertian lain dari keamanan informasi adalah upaya untuk mengamankan aset informasi dari segala ancaman yang mungkin terjadi untuk mengurangi resiko negatif yang diterima. Semakin banyak informasi yang disimpan di sebuah organisasi maka semakin banyak juga juga resiko yang akan terjadi seperti kerusakan, kehilangan atau juga informasi yang bersifat pribadi bisa tersebar ke pihak yang tidak bertanggung jawab (Lastyono, 2014). Keamanan informasi meliputi suatu mekanisme untuk mengontrol akses dan penggunaan *database* pada level objek, keamanan informasi pada pengguna, dimana pengguna tersebut memiliki akses informasi tertentu. Sedangkan Informasi adalah data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi yang menerimanya. Sumber dari informasi adalah data. Data merupakan bentuk jamak dari bentuk tunggal data-item. Data adalah kenyataan yang menggambarkan suatu kejadian-kejadian dan kesatuan nyata. Kejadian (*event*) adalah sesuatu yang terjadi pada saat tertentu. Kejadian kejadian nyata yang sering terjadi perubahan dari suatu nilai yang disebut dengan transaksi. Misalnya penjualan adalah transaksi perubahan nilai barang menjadi nilai uang. Kesatuan nyata adalah suatu objek nyata seperti tempat, benda, dan orang yang betul-betul ada dan terjadi (Afriyanto, 2017). Menurut Komalasari (2014),

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

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. Seringkali kelemahan keamanan informasi bergantung kepada manusia (pemakai dan pengelola).
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 recovery*), seringkali perusahaan tidak memiliki dokumen kebijakan dan prosedur tersebut.

Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara stimultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan (Riadi, 2016). *Computer security is a branch of technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption or natural disaster, while allowing the information and property to remain accessible and productive to its intended users* (Asma, 2014). *Managing information system security is increasingly concerning organizations, due to the continuous growing dependence of organizations on technology to conduct theirs businesses, to create a competitive advantage and achieving higher ROI* (Teresa, 2014).

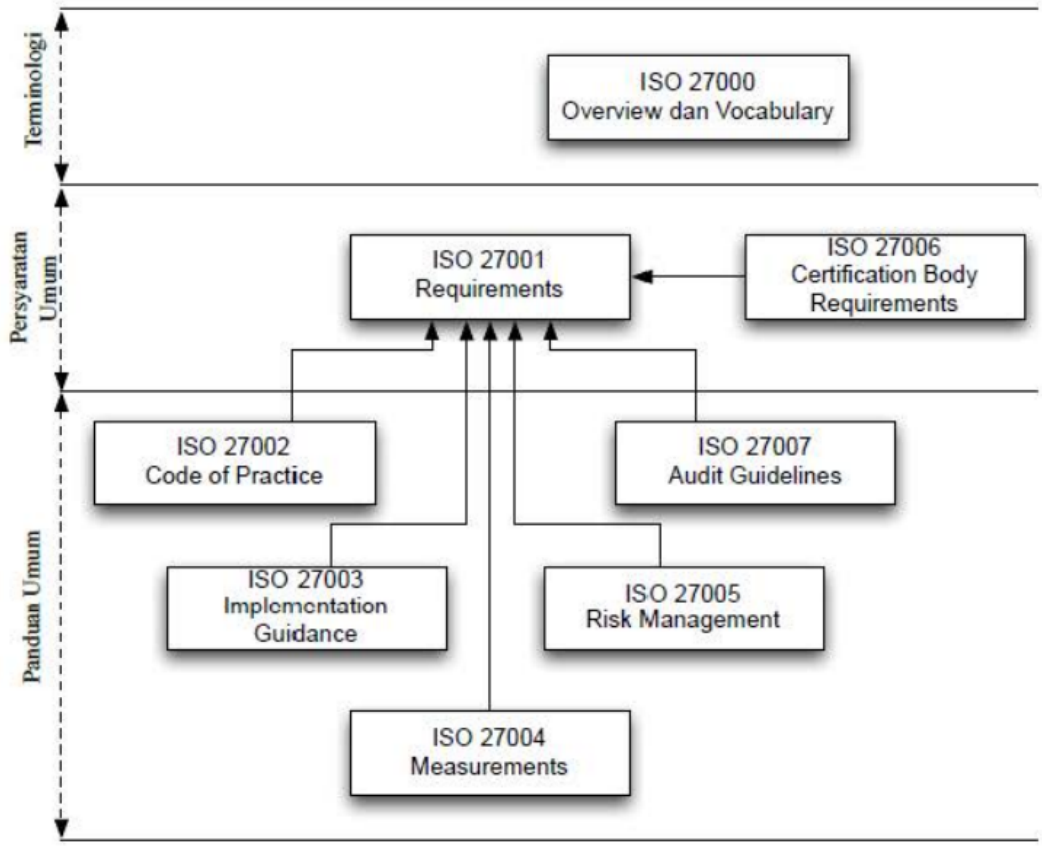
2.5 Metode Audit Operasional

Metode audit operasional berkaitan dengan penggunaan secara ekonomis dan efisien atas sumber daya pencapaian tujuan serta sasaran yang diterapkan (Steinbart, 2015). Menurut Sanyoto (2007), audit operasional memiliki 4 tahapan, yaitu :

1. Perencanaan
   a. Penetapan strategi audit
   b. Pelaksanaan survei pendahuluan
   c. Penyusunan rencana audit
2. Pekerjaan lapangan
   a. Penyusunan program audit, kriteria audit, dan instrumen pengumpulan bahan bukti.
   b. Pengumpulan data/bukti, *review,* uji, dan analisis.
   c. Penyusunan daftar masalah.
   d. Membahas masalah dengan pejabat lini/operasi.
   e. Analisis data dan melakukan observasi.
   f. Analisis antar hubungan dari hasil observasi.
   g. Penyiapan bahan untuk pembahasan dengan manajemen.
   h. Pembahasan dengan manajemen dari berbagai tingkat.
   i. Penuangan tanggapan manajemen dalam laporan.
3. Pelaporan
   a. Penerbitan *draft* laporan untuk didiskusikan dengan pihak manajemen.
   b. Analisis tanggapan manajemen dan memasukkannya ke dalam laporan.
   c. Penerbitan laporan final.
4. Tindak lanjut
   a. Analisis saling keterkaitan hasil-hasil audit atas suatu organisasi/unit organisasi.
   b. Penyiapan informasi untuk laporan berkala.
   c. Penyiapan informasi untuk penyusunan *database* bagi audit masa yang akan datang atau untuk keperluan lainnya.

2.6 Metode ISO 27001

International Standards Organization (ISO) mengelompokkan semua standar keamanan informasi ke dalam satu struktur penomoran, seperti pada gambar hubungan antar keluarga ISO/IEC 27000 sebagai berikut.



Gambar 2.1 Hubungan Antar Keluarga ISO/IEC 27000

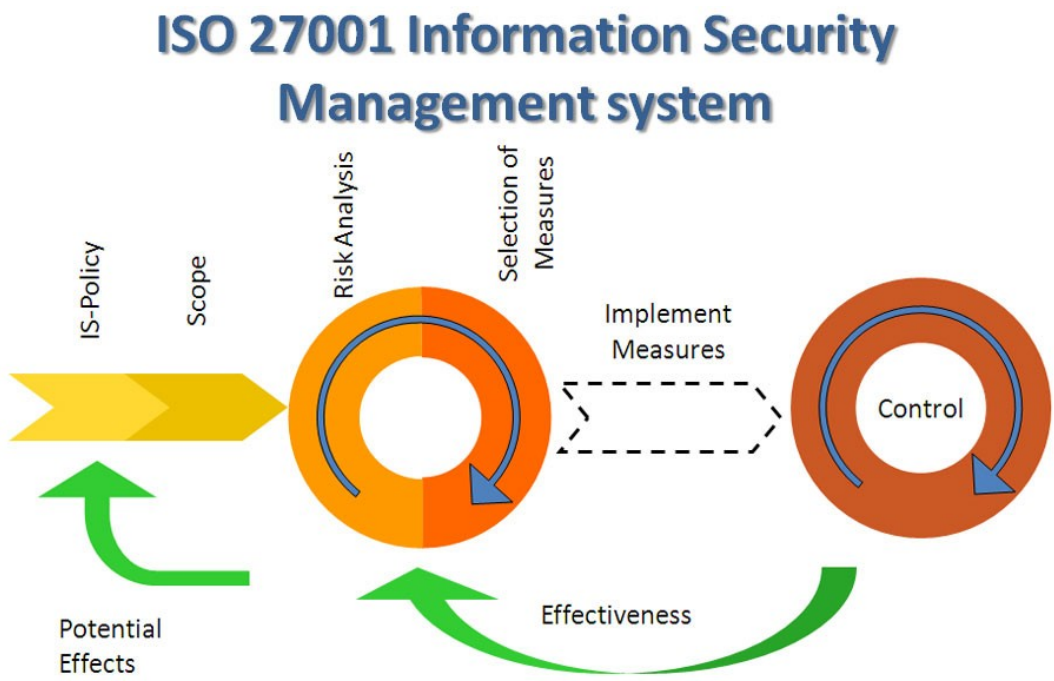
Sumber : (Chalifa, 2015)

Adapun beberapa standar pada seri ISO ini adalah sebagai berikut:

1. ISO 27000: berisi tentang dokumen defenisi-defenisi keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.
2. ISO 27001: berisi aspek-aspek pendukung tentang realisasi serta implementasi dari sistem manajemen keamanan informasi perusahaan.
3. ISO 27002: berhubungan dengan dokumen ISO 27001, namun dalam dokumen ini terdapat panduan praktis dalam pelaksanaan dan implementasi dari sistem manajemen keamanan informasi perusahaan.
4. ISO 27003: panduan tentang implementasi dari sistem manajemen keamanan informasi perusahaan.

5. ISO 27004: dokumen yang berisi tentang matriks dan metode sebagai pengukuran terhadap keberhasilan dari implementasi sistem manajemen keamanan informasi.
6. ISO 27005: dokumen panduan dalam hal pelaksanaan manajemen resiko.
7. ISO 27006: dokumen panduan untuk sertifikasi sistem manajemen keamanan informasi perusahaan.
8. ISO 27007: dokumen sebagai panduan audit sistem manajemen keamanan informasi perusahaan.

Pada penelitian ini menggunakan ISO/IEC 27001 yang merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management Systems* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi diperusahaan. *ISO/IEC 27001 is another widely-adopted InfoSec standard, which helps to determine the InfoSec status and degree of compliance with security policies and standards adopted by the business* (Cheuk, 2016). Kontrol keamanan berdasarkan ISO/IEC 27001 terdiri dari 11 klausul kontrol keamanan (*security control clauses*), 39 objektif kontrol (*control objectives*) dan 133 kontrol keamanan/kontrol (*controls*). ISO 27001 menyediakan berbagai macam kerangka kerja untuk netralitas penggunaan teknologi, netralitas dari sistem manajemen pengelolaan rekanan yang lebih memungkinkan suatu organisasi dalam memastikan bahwa pengukuran keamanan informasi sudah benar-benar efektif. Hal ini sudah termasuk dari sisi kemampuan dalam mengakses data secara berkelanjutan, adanya kerahasiaan dan integritas terhadap informasi yang sudah dimilikinya dan berbagai kebutuhan dari pihak-pihak yang berkepentingan demikian pula dengan kesesuaian hukumnya. Berikut ini merupakan skema sistem manajemen keamanan informasi pada ISO 27001.



Gambar 2. 2 Skema Sistem Manajemen Keamanan Informasi Pada ISO 27001

Penerapan ISO 27001 sebagai jawaban atas persyaratan hukum dan kemungkinan-kemungkinan terbesar terhadap adanya ancaman keamanan seperti:

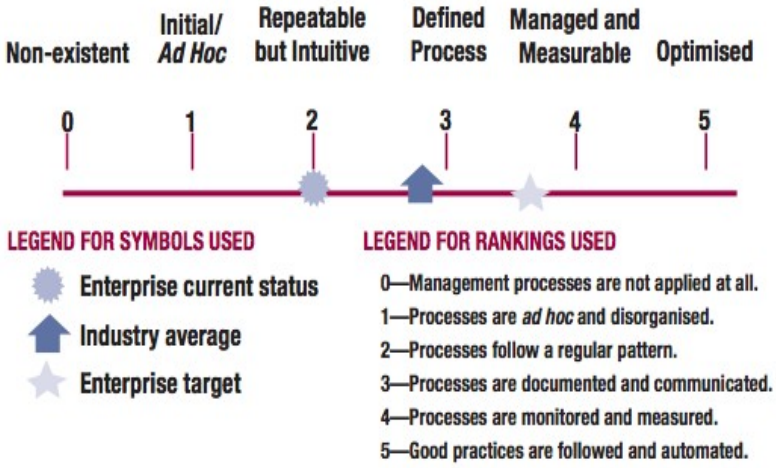
1. Perusakan / terorisme.
2. Ancaman dari kebakaran.
3. Kesalahan dalam hal penggunaan (*human errors*).
4. Pencurian data.
5. Serangan yang telah diakibatkan oleh virus-virus komputer berbahaya.

ISO 27001 telah disusun agar semakin mudah untuk melengkapi dengan standar sistem manajemen lainnya, seperti ISO 9001 dan ISO 14001. Meskipun dari beberapa klausul tertentu terdapat perbedaan, secara umum elemen-elemen yang sudah ada termasuk dari dokumentasi, persyaratan audit dan tinjauan manajemen, lebih memungkinkan terhadap suatu organisasi untuk mengembangkan secara lebih luas tentang integrasi sistem manajemen. Meskipun komunikasi modern sebenarnya membutuhkan adanya suatu perantara dan itu berarti bahwa sebagian besar dari sistem ISMS memang lebih mengutamakan pada ICT, ISO 27001

adalah penerapan yang sangat seimbang terhadap bentuk-bentuk informasi, seperti catatan-catatan, gambar-gambar, dan berbagai percakapan-percakapan yang tersaji dalam bentuk kertas.

2.7 Model *Maturity Level*

Salah satu alat pengukur dari kinerja suatu sistem teknologi informasi adalah model tingkat kematangan (*maturity level*). Model *maturity level* digunakan untuk mengontrol proses-proses teknologi informasi dengan metode penilaian. Tujuannya adalah organisasi dapat mengetahui posisi *maturity level* teknologi informasi saat ini dan organisasi dapat terus menerus berkesinambungan dan berusaha meningkatkan tingkatannya sampai tingkat tertinggi agar aspek *governance* terhadap teknologi informasi dapat berjalan dengan lancar. Tingkat kemampuan pengelola TI pada skala *maturity level* dibagi menjadi 6 *level* yang dapat dilihat pada gambar 2.3.



Gambar 2.3 Model *maturity level*

Keterangan masing-masing level sebagai berikut.

1. Level 0 (*non existent*)

Pada level ini, perusahaan sama sekali tidak perduli terhadap pentingnya teknologi informasi unuk dikelola secara baik oleh manajemen.

2. Level 1 (*initial*)
   Pada level ini, perusahaan secara aktif melakukan penerapan dan implementasi teknologi informasi sesuai dengan kebutuhan-kebutuhan mendadak yang ada, tanpa didahului dengan perencanaan sebelumnya.
3. Level 2 (*repeatable*)
   Pada level ini, perusahaan telah memiliki pola yang berulang kali dilakukan dalam manajemen aktivitas terkait dengan tata kelola teknologi, namun keberadaannya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidak konsistenan.
4. Level 3 (*define*)
   Pada level ini, perusahaan telah memiliki prosedur baku formal dan tertulis yang telah di sosialisasikan ke segenap jajaran dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari.
5. Level 4 (*manage*)
   Pada level ini, perusahaan telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun obyektif kinerja setiap penerapan aplikasi teknologi informasi yang ada.
6. Level 5 (*optimize*)
   Pada level yang terakhir, perusahaan telah mengimplementasikan tata kelola teknologi informasi yang mengacu pada "*best practice*".

Tabel 2.1 *Maturity level*

Indek Kematangan	**Level Kematangan**
0 – 0.49	0 – *Non-Existent*
0.50 – 1.49	1 – *Initial / Ad Hoc*
1.50 – 2.49	2 – *Repeatable But Intutitive*
2.50 – 3.49	3 – *Defined Process*
3.50 – 4.49	4 – *Managed and Measurebel*
4.50 – 5.00	5 – *Optimized*

2.8 Studi Literatur

Studi literatur dilakukan dengan cara mempelajari literatur-literatur baik yang berupa buku (*text book*), jurnal, dan artikel ilmiah, maupun *website* yang

berhubungan dengan ISO 27001, keamanan informasi, dan proses audit. Berikut ini akan dijelaskan studi literatur yang menjadi referensi penelitian ini.

Tabel 2.2 Sumber Studi Literatur

NO	NAMA	JURNAL/TAHUN	KETERANGAN
1	Fine Ermana	Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR Jatim/2014.	Mengingat pentingnya informasi, maka kebijakan tentang pengamanan informasi harus mencakup sekurang-kurangnya terdapat prosedur pengelolaan aset, prosedur pengelolaan sumber daya manusia, prosedur pengamanan fisik danlingkungan, prosedur pengamanan *logical security*, prosedur pengamanan operasional teknologi informasi dan prosedur penanganan insiden dalam pengamanan informasi. Untuk itu diperlukan audit keamanan sistem informasi pada PT. BPR JATIM untuk memastikan keamanan informasi diterapkan sesuai dengan prosedur standar ISO 27001.
2	Riawan Arbi Kusuma	Audit Keamanan Sistem Informasi	Diperlukan audit keamanan sistem informasi pada

		Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta/2014.	Universitas Islam Negeri Sunan Kalijaga Yogyakarta untuk memastikan keamanan informasi diterapkan sesuai prosedur.
3	Firzah Abdullah Basyarahil	Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 Pada Direktorat Pengembangan Teknologi Dan Sistem Informasi (DPTSI) ITS Surabaya/2017.	Pengelolaan Informasi merupakan salah satu aspek dalam Good University Governance, termasuk kualitas dan keamanan pengelolaan informasi. Salah satu upaya yang dapat dilakukan untuk meningkatkan kualitas dari keamanan informasi, kementrian Kominfo membuat alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Penggunaan Indeks KAMI ini juga diikuti dengan penerapan ISO 27001 sebagai standar keamanan internasional

			yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif.

Perbedaan penelitian dengan literatur :

1. Permasalahan yang dikaji dalam penelitian ini berfokus pada audit pada SMKN 1 Pugung menggunakan metode ISO 27001.
2. Pada pengukuran tingkat kematangan dilakukan dengan pemetaan terhadap klausul yang berkaitan dengan sistem keamanan informasi pada SMKN 1 Pugung.