Tabel 2-1 Klausal Manajemen

KLAUSAL
1. Scope
2. Normative references
3. *Terms and definition*
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Selain *klausal-klausal* tersebut, terdapat 114 kontrol yang terangkum dalam 14 domain kontrol pada bagian *Annex A* dokumen ISO 27001:2013 yang dapat di*implementasi*kan sesuai kebutuhan organisasi, antara lain:

Tabel 2-2 Kontrol dan Tujuan ISO 27001

No	Kontrol Area	Tujuan Kontrol
A.5	*Information Security Policies*	*Management Direction For Information Security*
A.6	*Organization Of Information Security*	*Organization Of Information Security*
		Internal Organization
		Mobile Devices And Teleworking
A.7	*Human Resource Security*	*Prior To Employment*
		During Employment
		Termination And Change Of Employment
A.8	*Asset Management*	*Responsibility For Assets*
		Information Classification
		Media Handling

persyaratan ISO 27001:2013 di klausal 6.1.3. Jika ISO 27001:2005 mencakup 133 kontrol dalam 11 area kontrol, versi ISO 27001:2013 memuat 114 kontrol dalam 14 area kontrol sebagai berikut:

Tabel 2-3 Domain ISO 27001:2013

No	Domain ISO 27001:2013
A.5	*Security Policies*
A.6	*Organisation of Information Security*
A.7	*Human Resource Security*
A.8	*Asset Management*
A.9	*Access Control*
A.10	*Access Control*
A.11	*Physical and Environmental Security*
A.12	*Operations Security*
A.13	*Communications Security*
A.14	*Systems Acquisition, Development and Maintenance*
A.15	*Supplier Relationships*
A.16	*Information Security Incident Management*
A.17	*mation Security Aspects of Business Continuity Management*
A.18	*Compliance*

2.5 Sistem Manajemen Keamanan Informasi

Sejak tahun 2005, Organisasi Internasional untuk Standarisasi (ISO) telah mengembangkan sejumlah standar tentang *Information SecurityManagement System (ISMS)* atau Sistem Manajemen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan.

Standar SMKI ini dikelompokkan sebagai keluarga atau seri ISO 27000 yang terdiri dari:

1. ISO/IEC 27000:2014 – *ISMS Overview and Vocabulary*
2. ISO/IEC 27001:2013 – *ISMS Requirements*
3. ISO/IEC 27002:2013 – *Code of Practice for ISMS*

manajemen tersebut. Seberapa bagusnya pengembangan atau kapabilitas manajemen tergantung pada tercapainya tujuan-tujuan. COBIT sebagai contoh adalah ada beberapa proses dan sistem kritikal yang membutuhkan manajemen keamanan yang lebih ketat dibanding proses dan sistem lain yang tidak begitu kritikal. Di sisi lain, derajat dan kepuasan pengendalian yang dibutuhkan untuk diaplikasikan pada suatu proses adalah didorong pada selera resiko *Enterprise* dan kebutuhan kepatuhan yang diterapkan.

Penerapan yang tepat pada tata kelola TI di suatu lingkungan *Enterprise*, tergantung pada pencapaian tiga aspek *maturity* (kemampuan, jangkauan dan kontrol). Peningkatan *maturity* akan mengurangi resiko dan meningkatkan efisiensi, mendorong berkurangnya kesalahan dan meningkatkan kuantitas proses yang dapat diperkirakan kualitasnya dan mendorong efisiensi biaya terkait dengan penggunaan sumber daya TI.

Maturity model dapat digunakan untuk memetakan :

1. Status pengelolaan TI perusahaan pada saat itu.
2. Status standart industri dalam bidang TI saat ini (sebagai pembanding)
3. Status standart internasional dalam bidang TI saat ini (sebagai pembanding)
4. Strategi pengelolaan TI perusahaan (ekspetasi perusahaan terhadap posisi pengelolaan TI perusahaan).

Tabel 2-4 *Maturity level*

Maturity level	***Practice***
Level 0 *(Non-existent)*	Perusahaan tidak mengetahui sama sekali proses teknologi informasi di perusahaannya
Level 1*(Initial Level)*	Pada level ini, organisasi pada umumnya tidak menyediakan lingkungan yang stabil untuk mengembangkan suatu produk baru. Ketika suatu organisasi kelihatannya mengalami kekurangan pengalaman manajemen, keuntungan dari mengintegrasikan pengembangan produk tidak dapat ditentukan dengan perencanaan yang tidak efektif, respon sistem. Proses pengembangan tidak

Tabel 2-5 *Maturity Index*

Maturity Indeks	*Maturity level*
4.51 – 5.00	5 – Dioptimalisasi *(Optimised)*
3.51 – 4.50	4 – Diatur *(Manage and Measurable)*
2.51 – 3.50	3 – Ditetapkan *(Defined)*
1.51 – 2.50	2 – Dapat diulang *(Repeatable but Intuitive)*
0.51 – 1.50	1 – Inisialisasi *(Initial/Ad Hoc)*
0.00 – 0.50	0 – Tidak ada *(Non-Existent)*

2.15 *Analisa Kesenjangan (Gap Analisys)*

Analisis kesenjangan adalah alat bisnis dan metode penilaian yang berfokus pada kesenjangan antara kinerja perusahaan saat ini dan kinerja yang diinginkan. Analisis kesenjangan mengevaluasi kinerja aktual saat ini dan upaya perbaikan yang diperlukan untuk menutup kesenjangan kinerja masa depan yang diinginkan. Manfaat dari Analisis kesenjangan ini adalah membantu perusahaan yang kinerjanya kurang baik karena tidak efisiennya penggunaan sumber daya atau kegagalan untuk berinvestasi dengan benar dan meningkatkan produksi serta kinerja (Mollick, 2008)

Selain itu, manfaat lain dari Analisis kesenjangan adalah dapat mengukur waktu, uang, dan sumber daya yang dibutuhkan untuk memenuhi potensi organisasi dan mencapai keadaan yang diinginkan.

2.16 Penelitian Sebelumnya

Dalam studi literatur yang dilakukan, penulis mengambil beberapa referensi yang dilakukan oleh penelitian sebelumnya yang berkaitan dengan topik penelitian yang penulis lakukan.

Tabel 2-6 Penelitian Terkait

No	Peneliti	Masalah	Metode	Hasil
1	Lusi Anggarini	Audit Keaman Sistem Informasi Perpustakaan Kota Yogyakarta	Lingkup Audit 7 *klausal* yaitu Kebijakan Keamanan,	Penelitian menghasilkan temuan Sistem Informasi

Tabel 3-1 Penilaian *Gap Analisys*

Nilai	Keterangan
1	Kontrol persyaratan tidak di*implementasi*kan atau direncanakan (Pasif).
2	Kontrol direncanakan namun tidak dilaksanakan (Reaktif).
3	Kontrol di*implementasi*kan sebagian, sehingga efek secara penuh tidak ditimbulkan (Penerapan kerangka kerja dasar).
4	Kontrol persyaratan di*implementasi*kan, namun pengukuran, *checklist*, dan perbaikan tidak dilakukan (Terdefinisi dan konsisten).
5	Kontrol di*implementasi*kan dan pengukuran, *checklist* dan perbaikan, dilakukan secara berkala (Terkelola dan terstruktur).

3.1.9 *Risk Assessment*

Risk assessment dilakukan setelah melakukan *gap analisys, risk assessment* bertujuan untuk melakukan penilaian resiko yang mungkin terjadi dari tahap sebelum itu. Resiko yang muncul dan kemungkinan untuk mengancam keamanan informasi dan pengelolaannya. Langkah *risk assessment*, yaitu dilakukan identifikasi aset, identifikasi kerawanan dan ancaman, menentukan prioritas resiko yang akan dikendalikan, menentukan kontrol apa saja yang dapat dilakukan untuk mengendalikan resiko, dan mengawasi resiko.

Adapun analisis yang akan dilakukan mengacu pada ISO 27001 berisi identifikasi kelengkapan aset, ketersediaan informasi yang digunakan apakah telah sesuai dengan permintaan lembaga yang berwenang, kerahasiaan menyangkut apakah informasi dapat diproses oleh pihak yang tidak berwenang, keamanan informasi mengenai *Confidentiality, Integrity, dan Availability (CIA).*

3.1.10 Menentukan Kontrol

Proses menentukan kontrol yang dipilih berdasarkan kontrol objektif dari ISO/IEC 27001. Kontrol ini didapatkan berdasarkan hasil identifikasi kerawanan dan ancaman serta dampak yang terjadi sehingga didapatkan rekomendasi yang akan menutupi celah-celah keamanan informasi yang ada.

Terdapat 14 domain dan 34 kontrol objektif didalam standarisasi ISO 27001:2013 berdasarkan lampiran A *(Annex A),* adapun domain dan kontrol objektif tersebut adalah sebagai berikut:

Tabel 3-2 Kontrol Area ISO 27001:2013

NO	KONTROL AREA	TUJUAN KONTROL
A.5	*Information Security Policies*	*Management Direction For Information Security*
A.6	*Organization Of Information Security*	*Organization Of Information Security*
		Internal Organization
		Mobile Devices And Teleworking
A.7	*Human Resource Security*	*Prior To Employment*
		During Employment
		Termination And Change Of Employment
A.8	*Asset Management*	*Responsibility For Assets*
		Information Classification
		Media Handling
A.9	*Access Control*	*Business Requirements Of Access Control*
		User Access Management
		User Responsibilities
		System And Application Access Control
A.10	*Cryptography*	*Cryptographic Controls*
A.11	*Physical And Environmental Security*	*Secure Areas*
		Equipment
A.12	*Operations Security*	*Operational Procedures And Responsibilities*
		Protection From Malware
		Backup
		Logging And Monitoring
		Control Of Operational Software
		Technical Vulnerability Management
		Information Systems Audit Considerations

4.3.2 Penilaian Resiko *(Risk Assessment)*

4.3.2.1 Identifikasi Aset

Tabel 4-1 Identifikasi Aset

No	Asset	Pemilik	Alokasi	Lokasi
Aset Perangkat Keras				
1	*Virtual Server Machine*	IT	*Internal*	Ruang *Server* lantai 10
2	*Router*	IT	*Internal*	Ruang *Server* lantai 10
3	*Switch*	IT	*Internal*	Ruang *Server* lantai 10
4	*Access Point*	IT	*Internal*	Ruang *Server* lantai 10
5	*Controler Wifi*	IT	*Internal*	Ruang *Server* lantai 10
6	*Firewall*	IT	*Internal*	Ruang *Server* lantai 10
7	*Proxy*	IT	*Internal*	Ruang *Server* lantai 10
8	*Server storage*	IT	*Internal*	Ruang *Server* lantai 10
9	*PC,laptop*	IT	*Internal*	Ruang *Server* lantai 10
10	*UPS*	IT	*Internal*	Ruang *Server* lantai 10
11	*CCTV*	IT	*Internal*	Ruang *Server* lantai 10
12	*AC*	Aset	*Internal*	Ruang *Server* lantai 10
13	*Access Door*	IT	*Internal*	Ruang *Server* lantai 10
Aset Perangkat Lunak				
10	*Sistem Operasi*	IT	*Internal*	Ruang *Server* lantai 10
11	*Anti virus*	IT	*Internal*	Ruang *Server* lantai 10
12	*Website*	IT	*Internal*	Ruang *Server* lantai 10
13	*Email server*	IT	*Internal*	Ruang *Server* lantai 10
14	*MRTG (multi router traffic grapher)*	IT	*Internal*	Ruang *Server* lantai 10
15	*ISP*	Non IT	*Internal*	Ruang *Server* lantai 10

4.3.2.1 Identifikasi Ancaman

Tabel 4-2 Hasil Identifikasi Ancaman

No	Ancaman *(Threats)*	Kode
1	Serangan *virus, worm, malware*	T1
2	Penerobosan oleh pihak eksternal melalui portal *web* dan IP Publik	T2
3	Akses ilegal	T3
4	*Hacker*	T4
5	Kebakaran	T5
6	Bencana alam (gempa, banjir)	T6
7	Kebakaran	T7

4.3.2.2 Identifikasi Kerawanan

Tabel 4-3 Hasil Identifikasi Kerawanan

No	Kerawanan *(Vulnerability)*	Kode
1	Persyaratan *sharing password*, *Password* masih ada yang menggunakan *password default* dari *vendor* sehingga ada kemungkinan disalahgunakan oleh orang yang tidak berhak	V1
2	Tidak adanya *petching* dan *update OS atau software yang end of support* dibeberapa *server*	V2
3	Proses *maintenance* dan *monitoring* tidak berjalan tepat waktu terkendala kurangnya *man power*	V3
4	*Reneual license* yang tertunda mengkibatkan perangklat lunak dan perangkat keras menjadi tidak terupdate	V4
5	Konfigurasi sistem yang masih menggunakan sandi bawaan yang dikonfigurasi oleh *vendor*.	V5

No	Kerawanan *(Vulnerability)*	Kode
6	Ada beberapa perangkat yang tidak dapat terkoneksi dengan aktif direktori sehingga timbul celah untuk penyalahgunaan *policy* contoh perangkat *BYOD (bring your own divice)*	V6
7	Perubahan tidak dilakukan secara berkala hanya ketika diperlukan	V7

4.4 Persiapan Audit

Pada tahap persiapan audit langkah-langkah yang dilakukan penyusunan *audit working plan* dan membuat pertanyaan yang diajukan pada *auditee.* Hasil dari tahap ini jadwal kerja audit dan materi kuesioner.

4.3.1 Penyusunan *Audit Working Plan*

Hasil dari penyusunan *audit working plan* berupa Tabel yang berisi serangkaian aktivitas yang dilakukan selama audit berlangsung. Dalam melaksanakan audit keamanan sistem informasi dilakukan secara bertahap. Dari kegiatan yang paling awal yaitu studi literatur hingga kegiatan akhir dari pelaksanaan audit keamanan informasi pada Divisi MIS Yayasan Tarumanagara yaitu penyusunan laporan hasil audit. Untuk lebih detailnya dapat dilihat pada Tabel 4-4 dibawah ini.

Tabel 4-4 *Audit Working Plan*

No	Kegiatan	Bulan															
		April				Mei				Juni				Juli			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur																
2	Penentuan ruang lingkup																
3	Identifikasi proses bisnis																
4	*Observasi* dan wawancara																
5	*Checklist* kelengkapan dokumen																

No	Kegiatan	Bulan															
		April				Mei				Juni				Juli			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
7	*Risk assessment*																
8	Identifikasi aset																
9	Identifikasi kerawanan																
10	Menetepakan kontrol																
11	Penyusunan daftar temuan																
12	Analisis rekomendasi																
13	Penyusunan laporan akhir																

4.3.2 Penyampaian Kebutuhan Data

Dalam proses penyampaian kebutuhan data, *audito*r memberikan *list* kebutuhan data-data yang digunakan selama proses audit kepada *auditee*. *List* kebutuhan data digunakan untuk menunjang proses audit. Kebutuhan data bisa dilihat pada Tabel 4-5.

Tabel 4-5 Permintaan Kebutuhan Data

No	Data Yang Diperlukan	Ketersediaan Data		Keterangan	Tanda Tangan	
		Ada	Tidak Ada		*Auditee*	Auditor
1	Profil *Divisi MIS*	√				
2	Struktur Organisasi Yayasan Tarumanagara	√				
3	Job Desk Staf *Divisi MIS*	√				
4	Alur Proses Bisnis *Divisi MIS*	√				
5	Dokumen Penyusunan IT Plan	√				

4.5 Pelaksanaan Audit

Pada pelaksanaan audit di Divisi MIS Yaysan Tarumangara, Jakarta ada beberapa tahap yang dilakukan yaitu wawancara dan *observasi*, pemeriksaan data dan bukti, melakukan penilaian *Maturity level* terhadap kuesioner serta penghitungan *gap* analisis *maturity*. *Output* yang dihasilkan dari tahap tersebut adalah pertanyaan dan jawaban tabel hasil pengisian *kuesioner*, tabel *maturity*, *tabel (gap)* Analisis dan foto bukti hasil audit yang dapat dilihat pada lampiran 10.

4.5.1 Wawancara, Pengisian Kuesioner dan *Observasi*

Pada proses wawancara dan *observasi*, *auditor* melakukan wawancara dan *observasi* berdasarkan pertanyaan yang telah dibuat. Wawancara dilakukan kepada pihak yang terlibat di dalamnya yaitu *auditee*. Dalam penentuan *auditee* didapat dari analisa tabel RACI. *Auditee* adalah penanggungjawab atau *responsibility* dari proses keamanan. Tabel RACI dapat dilihat pada Tabel 4-6.

Tabel 4-6 RACI

Bagian / ***Klausal***	**Kepala *Divisi***	**Staf Penyusunan It Plan**	**Staf Pengadaan Lisensi It**	**Staf *Hardware***	**Staf *Software***
Klausal A.5 Kebijakan Keamanan Informasi	A/R	I	I/C	R	R
Klausal A.9 Kontrol Akses	I/A/C	I/C	I	I	I
Klausal A.11 (Keamanan Fisik dan Lingkungan	I/C	I	I/C	I	I
Klausal A.12 (Keamanan Operasional)	A	I	I/C	R	R
Klausal A.13 Keamanan Komunikasi	A	I	I	R	R

4.5.2 Penilaian Tingkat Kematangan

Penilaian kematangan pada yang dilakukan oleh auditor mengacu pada *Capability Maturity Model for Integration (CMMI)* Cobit. Untuk menilai tingkat kematangan pada penerapan pengelolaan kemanan informasi, dapat dilihat pada Tabel 4-7.

Pengukuran tingkat kematangan *(Maturity level)* berdasarkan pengisian kuesioner yang diberikan kepada staf Divisi MIS berdasarkan kontrol ISO 27001.

Tingkat kematangan proses dapat diukur menggunakan alat ukur *maturity* dengan rumus :

$$Index\ Maturity = \frac{\text{Jumlah Jawaban}}{\text{Jumlah Soal Kontrol}}$$

Tabel 4-7 Penilaian Tingkat Kematangan

Level	Status	Description
0	*Non-Existent*	*Process is not applied at all*
1	*Initial/ad hoc*	*Process is ad hoc and disorganized*
2	*Repeatable But Intuitive*	*Process follow regular pattern*
3	*Difined Process*	*Process is documented and communicated*
4	*Managed and Measurable*	*Process is Monitored measured*
5	*Optimized*	*Process followbest practices and automated*

4.5.3 Analisis Temuan

Analisis temuan dibuat berdasarkan pengukuran *Maturity level* sebelumnya. Analisis temuan tujuannya untuk menentukan strategi penerapan pengembangan kontrol keamanan. Hasil dari Analisis temuan tersebut dijadikan acuan untuk perbaikan kontrol keamanan. Berikut hasil analisis temuan dari

keseluruhan *Maturity level* : Klausa A.5 Kebijakan Keamanan, Klausal A.9 Kontrol Akses, Klausa A.11 Keamanan Fisik dan Lingkungan, Klausal A.12 Keamanan Operasi A.13 Keamanan Komunikasi

Tabel 4-8 Hasil Penilaian Maturity Seluruh Klausal

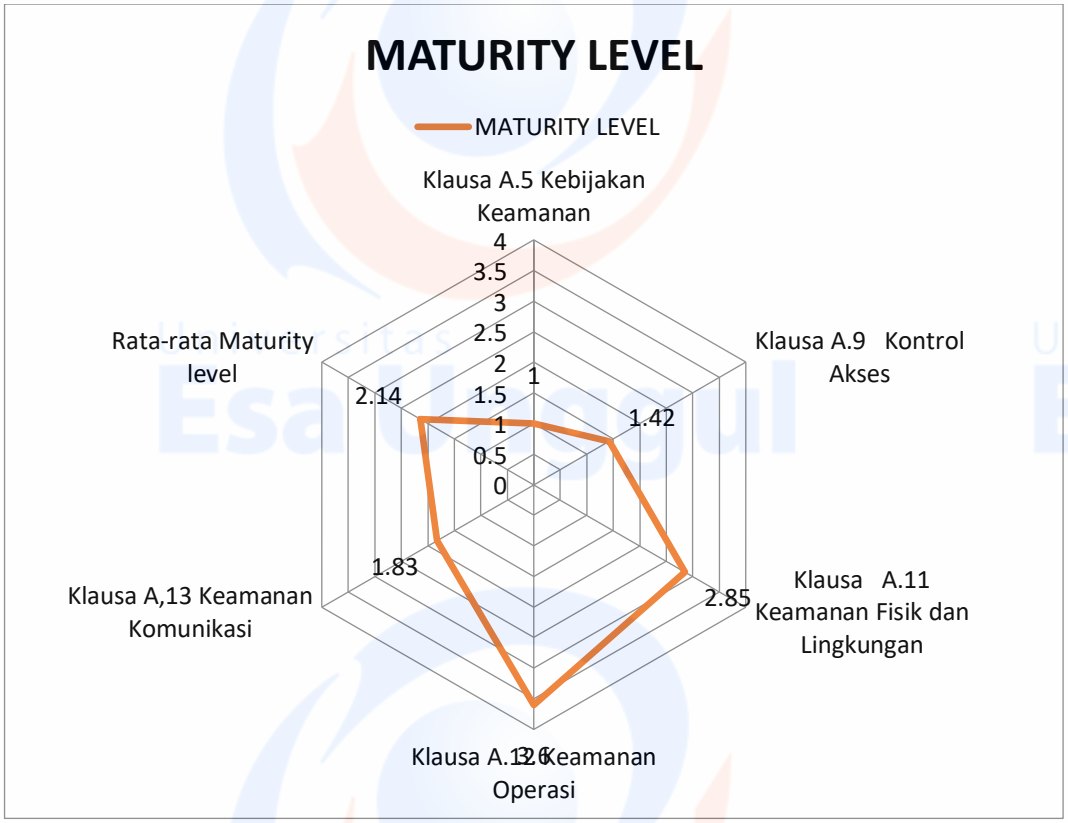
KLAUSAL	*MATURITY LEVEL*
Klausa A.5 Kebijakan Keamanan	1
Klausa A.9 Kontrol Akses	1.42
Klausa A.11 Keamanan Fisik dan Lingkungan	2.85
Klausa A.12 Keamanan Operasi	3.6
Klausa A,13 Keamanan Komunikasi	1.83
Rata-rata *Maturity level*	**2.14**

Hasil tabel 4-8 dapat dijelaskan bahwa :

a. Klausal A. 5 Kebijakan Keamanan dengan nilai tingkat kematangan 1 *(Initial/Ad Hoc)* artinya mulai adanya pemahaman tentang pengelolaan keamanan informasi. Penerapan pengamanan masih bersifat *reaktif*, tidak teratur, tidak mengacu pada seluruh resiko yang ada tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan.
b. Klausal A. 9 Kontrol Akses dengan nilai kematangan 1.42 *(Initial/Ad Hoc)* artinya mulai adanya pemahaman tentang pengelolaan keamanan informasi. Penerapan pengamanan masih bersifat *reaktif*, tidak teratur, tidak mengacu pada seluruh resiko yang ada tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan.
c. Klausal A.11 Keaman Fisik dan Lingkungan dengan nilai kematangan 2.85 (ditetapkan/*Defined process*) proses telah di dokumentasikan dan dikomunikasikan, prosedur telah distandarisasi. Proses berada dalam keadaan diamanatkan.

d. Klausal A.12 Keamanan Komunikasi dengan nilai kematangan 3.6 (ditetapkan/*Defined process*) proses telah di dokumentasikan dan dikomunikasikan, prosedur telah disetandarisasi. Proses berada dalam keadaan diamanatkan.
e. Klausal A.13 Keamanan Komunikasi dengan nilai kematangan 1.83 *(repeatable but intuitive)* proses mengikuti pola yang teratur dimana prosedur diikuti pegawai/karyawan lain tetapi tidak ada peraturan formal yang digunakan sebagai acuan.

Jadi nilai rata-rata yang didapat dari seluruh klausal yaitu 2.14 yang artinya tingkat kematangan pengelolaan keamanan informasi pada Divisi MIS *Repeatable but Intuitive* perusahaan telah memiliki kebiasaan yang terpola untuk merencanakan dan mengelola tata kelola TI dan dilakukan secara berulang-ulang secara reaktif, namun belum melibatkan prosedur dan dokumen formal.



Gambar 4-4 Hasil Penilaian *Maturity* Seluruh Klausal