

BAB II

LANDASAN TEORI

2.1 Penelitian Terdahulu

Penelitian terkait evaluasi sistem keamanan dilakukan dengan berbagai *framework* yang berbeda. Salah satunya adalah *framework* Indeks KAMI 4.2. Penelitian terdahulu yang serupa menjadi referensi dalam penyusunan penelitian ini. Sebanyak 15 penelitian terdahulu telah dikumpulkan untuk studi literatur. Pencarian penelitian terdahulu dilakukan dengan menggunakan Aplikasi Mendeley, Google Scholar, dan Jurnal Infosys.

Tabel 2.1 Rangkuman Penelitian Terdahulu

1 [10]	Penulis	Rizky Yulizar Rahman, Muhammad Said Hasibuan
	Nama Jurnal	Jurnal Fasilkom vol. 13, no. 2, pp. 181-187, Agustus 2023
	Judul	Evaluasi Keamanan Informasi Pada SMAN 1 Tanggamus Menggunakan indeks KAMI Versi 4.2
	Metode	Studi Literatur, Wawancara, Observasi, Indeks KAMI 4.2
2 [11]	Hasil	Hasil evaluasi menunjukkan bahwa tingkat kebutuhan perangkat elektronik mencapai nilai 20 pada indeks KAMI, yang setara dengan level I hingga level II. Nilai akhir penilaian adalah 245 dengan tingkat keamanan I.
	Penulis	Dicky Insan Khamil, Gusti Made Arya Sasmita, Anak Agung Ngurah Hary Susila
	Nama Jurnal	Jurnal Teknik Informatika dan Sistem Informasi vol. 9, no. 3, pp. 1948-1960, September 2022
	Judul	Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI 4.2 Dan ISO/ IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar)
3 [12]	Metode	Wawancara, Observasi, Kuesioner, <i>Checklist</i> untuk validasi, Indeks KAMI 4.2
	Hasil	Hasil evaluasi menunjukkan skor kategori Sistem Elektronik sebesar 34 (kategori tinggi) dan skor kategori Keamanan Informasi sebesar 190, yang menempatkan instansi pada status "Tidak Layak" untuk memenuhi standar atau kontrol ISO/IEC 27001, dengan tingkat kematangan terendah pada Tingkat I dan tertinggi pada Tingkat II+. Area Teknologi dan Keamanan Informasi memiliki penerapan terbaik, sementara area lainnya membutuhkan perbaikan agar sesuai dengan Kerangka Kerja Dasar, terutama di Area Pengelolaan Risiko dan Area Kerangka Kerja.
	Penulis	Muh. Faturachman, Hans F. Wowor, Stanley D.S. Karouw
	Nama Jurnal	E-Journal Teknik Informatika vol. 12, no. 1, pp. 1-8, 2017
	Judul	Implementasi Indeks KAMI di Universitas Sam Ratulangi
	Metode	Studi Literatur, Wawancara, Kuesioner, <i>Accidental Sampling</i> , Indeks KAMI 4.2

	Hasil	Hasil evaluasi menunjukkan nilai yang didapat adalah 191 dari nilai maksimum 588 sehingga sistem dinyatakan tidak layak untuk memenuhi kriteria yang diberikan oleh KAMI.
4 [13]	Penulis	Nabilla Diva Ramadhani, Widhy Hayuhardhika Nugraha Putra, Admaja Dwi Herlambang
	Nama Jurnal	Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer vol. 4, no. 5, pp. 1490-1498, Mei 2020
	Judul	Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang Menggunakan Indeks KAMI (Keamanan Informasi)
	Metode	Studi Literatur, Wawancara, Kuesioner, <i>Checklist Method</i> , Indeks KAMI 4.2
	Hasil	Hasil menunjukkan tingkat kelengkapan yang rendah dengan skor 195 ada di Level I hingga Level II. Hal ini menghasilkan beberapa rekomendasi perbaikan di berbagai bidang, seperti tata kelola, kerangka kerja, pengelolaan risiko, pengelolaan aset, teknologi, dan suplemen, guna meningkatkan keamanan informasi.
5 [14]	Penulis	Aprilian Lisa Maryanto, Moh Noor Al Azam, Aryo Nugroho
	Nama Jurnal	Jurnal SimanteC vol. 11, no. 1, pp. 1-12, Desember 2022
	Judul	Evaluasi Manajemen Keamanan Informasi pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks KAMI
	Metode	Studi Literatur, Analisis SWOT, Wawancara, Observasi Lapangan, Indeks KAMI 4.2
	Kesimpulan	Hasil evaluasi menunjukkan bahwa tingkat kematangan dan kelengkapan manajemen keamanan informasi berada pada level I hingga I+ dengan status "Tidak Layak" dan banyak pertanyaan berstatus "Tidak Dilakukan" atau "Dalam Perencanaan," sehingga direkomendasikan penerapan Kontrol ISO 27002:2013, termasuk membuat prosedur pertukaran informasi yang aman antara pengelola keamanan informasi dengan pihak internal maupun eksternal instansi.
6 [15]	Penulis	Faradhiya Aulia, Najwa Hamidah, Bintang Nuari, Reisa Permatasari
	Nama Jurnal	Seminar Nasional Teknologi dan Sistem Informasi (SITASI) 2023
	Judul	Analisis Keamanan Informasi Menggunakan Aplikasi Indeks KAMI pada Sekretariat DPRD Kabupaten Jombang
	Metode	Studi Literatur, Wawancara, Kuesioner, Indeks KAMI 4.2
	Hasil	Hasil evaluasi menunjukkan bahwa sistem elektronik berperan penting dalam keamanan informasi, meskipun telah diterapkan sebagian, masih terdapat ruang peningkatan dalam aspek pengelolaan risiko, kerangka kerja, tata kelola, teknologi, dan suplemen keamanan informasi, sehingga organisasi perlu mengambil langkah-langkah komprehensif untuk memperbaiki dan memperbarui suplemen keamanan informasi sesuai perkembangan teknologi.
7 [16]	Penulis	Eko Jhony Pranata, Muhammad Taufiq Nuruzzaman
	Nama Jurnal	<i>CyberSecurity</i> dan Forensik Digital vol. 5, no. 1, pp. 32-45, Mei 2022
	Judul	Optimasi Keamanan Informasi Menggunakan Manajemen Indeks Keamanan Informasi (KAMI) Studi Kasus: IBISA Purworejo
	Metode	Studi Literatur, Kuesioner, Simulasi, <i>Monitoring</i> , Indeks KAMI 4.2
	Hasil	Hasil evaluasi menunjukkan bahwa tingkat kematangan dan integritas keamanan informasi masih rendah karena belum sepenuhnya menerapkan persyaratan keamanan informasi. Namun, penggunaan teknologi <i>ManageEngine OpManager</i>

		membantu dalam menganalisis kelemahan dan perubahan konfigurasi aset informasi, sehingga tingkat kematangan berada pada level I hingga II. Perbaikan diperlukan untuk mencapai ambang batas minimum sertifikasi Level III+ sesuai standar ISO/IEC 27001:2018.
8 [17]	Penulis	I Putu Setyo Syahindra, Clara Hetty Primasari, Aloysius Bagas Pradipta Irianto
	Nama Jurnal	Jurnal Teknoinfo vol. 16, no. 2, pp. 165-182, Juli 2022
	Judul	Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi XYZ Menggunakan Indeks KAMI Dan ISO 27005 : 2011
	Metode	Studi Literatur, Wawancara, Kuesioner, Indeks KAMI, ISO/IEC 27005:2011
	Hasil	Hasil evaluasi menunjukkan sistem sangat bergantung pada penggunaan sistem elektronik dan memiliki tingkat kelengkapan yang "Cukup Baik" (457 poin) dalam pemenuhan standar ISO/IEC 27001. Namun, tingkat kematangan keseluruhan hanya mencapai III+, yang berarti sistem hanya memenuhi standar minimal ISO/IEC 27001.
9 [18]	Penulis	Reynaldo Adi Putra Pratama Gala, Rizal Sengkey, Charles Punusingon
	Nama Jurnal	Jurnal Teknik Informatika vol. 15, no. 3, pp. 189-198, Juli-September 2020
	Judul	Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI
	Metode	Studi Literatur, Wawancara, Kuesioner, <i>Accidental Sampling</i> , Indeks KAMI 3.1
	Hasil	Hasil evaluasi memperlihatkan bahwa Tingkat Kematangan Keamanan Informasi tergolong rendah dengan nilai 264 dari 645 dan belum memenuhi standar SNI ISO/IEC 27001:2013 sehingga perbaikan diperlukan di semua aspek, termasuk tata kelola, risiko keamanan, kerangka kerja, pengelolaan aset, teknologi, dan keamanan informasi.
10 [19]	Penulis	Hadiati Agus Pratiwi, Lily Wulandari
	Nama Jurnal	<i>Journal of Industrial Engineering & Management Research</i> vol. 2, no. 5, pp. 146-163, Oktober 2021
	Judul	Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor
	Metode	Studi Literatur, Wawancara, Indeks KAMI 4.0
	Hasil	Hasil evaluasi menunjukkan bahwa sistem elektronik tergolong strategis dengan skor 35. Kesiapan pengamanan informasi berada pada tahap "Pemenuhan Kerangka Kerja Dasar" dengan tingkat kematangan level I+ hingga II. Area suplemen menunjukkan keterlibatan pihak ketiga sebesar 36%, perlindungan data pribadi sebesar 52%, dan keamanan layanan infrastruktur awan tidak digunakan, sehingga mendapatkan skor 0%.
11 [20]	Penulis	Rizki Dewantara, Bambang Sugiantoro
	Nama Jurnal	Jurnal Teknologi Informasi dan Ilmu Komputer (JTIK) vol. 8, no. 6, pp. 1137-1148, Desember 2021
	Judul	Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus : UIN Sunan Kalijaga Yogyakarta)
	Metode	Studi Literatur, Kuesioner, Simulasi, <i>Monitoring</i> , Indeks KAMI
	Hasil	Hasil evaluasi menunjukkan bahwa jaringan masih memiliki tingkat kelengkapan dan keamanan informasi yang rendah karena belum memenuhi semua persyaratan keamanan informasi. Tingkat

		kelayakan berada pada level I+ hingga II+, sehingga jaringan memerlukan perbaikan. Namun, penggunaan teknologi <i>Open Source</i> SIEM (OSSIM) dapat meningkatkan nilai indeks KAMI dengan menganalisis kelemahan dan perubahan konfigurasi aset informasi.
12 [21]	Penulis	Samsiana Firmayanti Rahayu, Dian Prawira, Ibnu Rusi
	Nama Jurnal	Coding : Jurnal Komputer dan Aplikasi vol. 09, no. 03, pp. 468-477, 2021
	Judul	Pengukuran Tingkat Keamanan Informasi Menggunakan Metode Indeks KAMI (Studi Kasus: Dinas Komunikasi dan Informatika Kota Pontianak)
	Metode	Studi Literatur, Kuesioner, Indeks KAMI 4.0
	Hasil	Hasil evaluasi menunjukkan bahwa sebagian besar aspek keamanan informasi belum diimplementasikan secara optimal dan berkesinambungan, meskipun beberapa divisi memiliki tingkat kematangan yang bervariasi dari level I+ hingga III+.
13 [22]	Penulis	Piski Sundari, Wella
	Nama Jurnal	Ultima InfoSys : Jurnal Ilmu Sistem Informasi vol. 12, no. 1, pp. 35-42, Juni 2021
	Judul	SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)
	Metode	Studi Literatur, Observasi, Wawancara, Pendekatan PDCA (<i>Plan – Do – Check – Act</i>), Indeks KAMI
	Hasil	Hasil evaluasi menunjukkan bahwa instansi belum siap atau "Perlu Perbaikan" dalam melindungi asetnya, sehingga rentan terhadap kejahatan yang dapat mengganggu layanan sistem informasi.
14 [23]	Penulis	Darmanto, Ar-Razy Muhammad, Rustiarni
	Nama Jurnal	Jurnal Informasi Interaktif vol. 9, no. 1, pp. 1-9, Januari 2024
	Judul	Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI 4.2 pada Politeknik Negeri Ketapang
	Metode	Studi Literatur, Wawancara, Observasi, Kuesioner, Indeks KAMI 4.2
	Hasil	Hasil evaluasi menunjukkan Politeknik Negeri Ketapang telah mencapai kategori tinggi dalam penggunaan sistem elektronik dengan skor 16 dari 50, tetapi meskipun Indeks KAMI menunjukkan tingkat kematangan II sampai II+ dengan skor 453 dari 645, perbaikan mendesak diperlukan untuk meningkatkan langkah-langkah pengamanan dan pengawasan serta meningkatkan kesadaran tanggung jawab pihak pengelola keamanan informasi.
15 [24]	Penulis	Yahya Dwi Wijaya
	Nama Jurnal	Jurnal Sistem Informasi dan Informatika (SIMIKA) vol. 4, no. 2, pp. 115-130, Agustus 2021
	Judul	Evaluasi Keamanan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013
	Metode	Studi Literatur, Wawancara, Kuesioner, Indeks KAMI 4.1
	Hasil	Hasil evaluasi menunjukkan bahwa sistem informasi Pasdeal mendapat predikat Baik dalam tingkat penerapan standar ISO 27001 dengan total nilai 591 dan sistem berada di tingkat kematangan III yang berarti beberapa perbaikan perlu dilakukan.

Tabel 2.1 menampilkan rangkuman penelitian terdahulu. Dari lima belas penelitian terdahulu, banyak perusahaan yang telah melakukan evaluasi

ditemukan memerlukan perbaikan pada tingkatan tertentu dan beberapa perusahaan lainnya ditemukan belum patuh terhadap ISO 27001. Dibandingkan dengan penelitian ini, beberapa aspek memiliki kesamaan dan juga perbedaan. Kesamaan yang dimiliki adalah metode yang digunakan untuk pengumpulan data. Hampir seluruh penelitian terdahulu melakukan wawancara untuk pengumpulan data. Hampir seluruh penelitian terdahulu melakukan wawancara untuk pengumpulan data. Perbedaan penelitian ini dengan penelitian-penelitian terdahulu adalah objek penelitian dan tingkat analisis yang dilakukan. Sebagian besar objek penelitian adalah instansi pemerintah dan sebagian lainnya adalah perusahaan swasta. Selain itu, tingkat analisis yang dilakukan berbeda-beda. Pada beberapa penelitian terdahulu, analisis dilanjutkan ke tingkat selanjutnya dengan menggunakan *framework* yang berbeda.

Dalam penelitian ini, kebaruan yang membedakan dengan penelitian-penelitian sebelumnya adalah objek penelitian dan kerangka kerja. Objek penelitian yang diteliti adalah perusahaan swasta dimana evaluasi menggunakan ISO 27001 umumnya dilakukan terhadap perusahaan negeri dan masih jarang dilakukan terhadap perusahaan swasta. Dari segi kerangka kerja, penelitian ini menerapkan Teknik Analisis Gallegos.

2.2 Teori

2.2.1 Keamanan Informasi

Keamanan informasi merupakan upaya melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, pengoperasian, perubahan, atau kerusakan oleh pihak yang tidak berwenang untuk menjamin kerahasiaan, integritas, dan kemudahan penggunaan [25]. Simons dalam Siregar menjelaskan bahwa keamanan informasi berkaitan dengan bagaimana kita dapat mencegah atau setidaknya mendeteksi adanya penipuan dalam sistem informasi di mana informasi itu sendiri tidak memiliki bentuk fisik. [26]. Dari kedua definisi tersebut, dapat disimpulkan bahwa keamanan informasi adalah usaha melindungi data sebagai aset penting bagi perusahaan atau organisasi untuk mencegah

kebocoran dan kehilangan, serta memastikan integritas informasi tersebut tetap terjaga.

Pada dasarnya, keamanan informasi memiliki tiga konsep dasar, yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan informasi (*availability*) [27]. Ketika informasi yang seharusnya bersifat rahasia dibaca oleh orang yang tidak berwenang, maka kerahasiaan informasi tersebut hilang (*loss of confidentiality*). Selanjutnya, informasi memiliki kemungkinan rusak saat ada perubahan yang tidak terduga akibat kesalahan pengguna, jaringan yang tidak aman hingga kerusakan yang disengaja. Ketika hal ini terjadi, informasi menjadi tidak utuh dan tidak valid (*loss of integrity*) untuk digunakan sebagai acuan dalam pengambilan keputusan. Terakhir, Ketika informasi hilang, terhapus, ataupun tidak bisa diakses, maka orang yang berwenang tidak memiliki ketersediaan informasi (*loss of availability*).

2.2.2 *International Organization for Standardization (ISO)*



Gambar 2.1 Logo *International Organization for Standardization (ISO)*

International Organization for Standardization (ISO) merupakan sebuah organisasi internasional non-pemerintah yang independen dengan keanggotaan 170 badan standar nasional [28]. ISO secara resmi berdiri di tahun 1947 dengan 67 orang komite yang terdiri dari kelompok ahli yang berfokus pada subjek tertentu. Kegiatan utama ISO adalah

menghasilkan standar internasional. Seluruh standar yang diterbitkan membantu membuat produk kompatibel, mengidentifikasi masalah keselamatan, serta memberikan ide dan solusi praktis [29].

Selama 75 tahun, ISO telah mengeluarkan banyak standar internasional. Hal ini sesuai dengan misi ISO yang mendukung pengembangan standarisasi dan kegiatan terkait lainnya dengan tujuan untuk mendukung perdagangan internasional, serta mendorong kerjasama global di bidang ilmu pengetahuan, teknologi, dan kegiatan ekonomi [30]. Per Bulan Desember 2023, ISO telah mempublikasikan lebih dari 25.000 standar internasional dan dokumen-dokumen terkait yang mencakup hampir seluruh sektor industri.

2.3 ISO/IEC 27001

ISO/IEC 27001 adalah standar internasional yang mengatur sistem manajemen keamanan informasi atau *Information Security Management Systems* (ISMS). Standar ini memberikan panduan kepada perusahaan dari berbagai ukuran dan dari semua sektor aktivitas untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi [31]. ISO/IEC 27001 membantu organisasi dan perusahaan untuk sadar akan risiko yang ada, serta mengidentifikasi kelemahan sistem secara proaktif. Pada awalnya, ISO/IEC 27001 diterbitkan untuk pertama kali di tahun 2013 dan lebih dikenal sebagai ISO/IEC 27001:2013. Namun, seiring dengan perkembangan teknologi dan meningkatnya kejahatan siber, pembaruan standar dilakukan agar ISO 27001 tetap relevan dengan kondisi saat ini. Oleh karena itu, ISO/IEC 27001:2022 diterbitkan.

Beberapa aspek diperbarui dalam ISO/IEC 27001:2022 [32]. Pertama, jumlah pengendalian keamanan informasi telah dikurangi dari 114 menjadi 93 dimana 24 digabungkan, 58 direvisi, 11 baru, dan 21 dihapus. Kedua, empat kategori keamanan baru, yaitu pengendalian organisasi, pengendalian orang, pengendalian fisik, dan pengendalian teknologi. Terakhir, lima atribut

pengendalian baru berupa tipe pengendalian, properti keamanan informasi, konsep keamanan siber, kemampuan operasional, dan domain keamanan.

2.4 Indeks Keamanan Informasi (KAMI)

Indeks KAMI (Keamanan Informasi) merupakan sebuah aplikasi untuk mengevaluasi tingkat kematangan dan kelengkapan penerapan ISO/IEC 27001 serta peta area tata kelola keamanan sistem informasi dalam suatu instansi pemerintah [33]. Aplikasi ini dibuat dengan menerapkan standar ISO/IEC 27001 dan terus diperbarui untuk menyesuaikan dengan pembaruan standar yang dilakukan ISO/IEC 27001. Proses evaluasi pada Indeks KAMI dilakukan melalui sejumlah pertanyaan di beberapa aspek [9], yaitu:

a. Kategori Sistem Elektronik

Aspek ini merupakan aspek terkait sistem yang digunakan dalam sistem, mulai dari sistem komunikasi, pengolahan data, kendali, hingga daya.

b. Tata Kelola

Aspek ini merupakan aspek terkait pengelolaan sistem keamanan informasi.

c. Pengelolaan Risiko

Aspek ini merupakan aspek terkait pengelolaan risiko yang dimiliki sistem keamanan informasi.

d. Pengelolaan Aset

Aspek ini merupakan aspek terkait pengelolaan aset atau data yang dimiliki sebuah organisasi atau perusahaan.

e. Kerangka Kerja

f. Aspek ini merupakan aspek terkait cara kerja sistem keamanan Teknologi Keamanan Informasi

Aspek ini merupakan aspek terkait teknologi yang digunakan dan keamanan informasi yang diterapkan dalam sistem.

g. Suplemen

Aspek ini merupakan aspek tambahan untuk mengamankan keterlibatan pihak ketiga penyedia layanan, keamanan layanan infrastruktur awan, dan perlindungan data pribadi.

2.5 Teknik Analisis Gallegos

Teknik Analisis Gallegos merupakan teknik analisis yang terdiri dari beberapa tahap [34], yaitu:

a. Penyusunan Rencana (*Planning*)

Dalam tahap ini, langkah pertama adalah menetapkan lingkup audit, objek yang akan diaudit, standar evaluasi hasil audit, dan berkomunikasi dengan manajemen organisasi terkait. Hal ini melibatkan analisis terhadap visi, misi, sasaran, dan tujuan objek yang akan diaudit, serta strategi dan kebijakan terkait. Aktivitas dalam penyusunan rencana meliputi penetapan ruang lingkup dan tujuan audit, pembentukan tim audit, pemahaman terhadap operasi bisnis klien, tinjauan kembali hasil audit sebelumnya, dan penyusunan program audit.

b. Penelitian Lapangan (*Field Work*)

Tahap ini melibatkan pengumpulan informasi melalui interaksi dengan pihak terkait. Pengumpulan data dapat dilakukan dengan berbagai metode seperti wawancara, kuesioner, atau survei di lokasi penelitian.

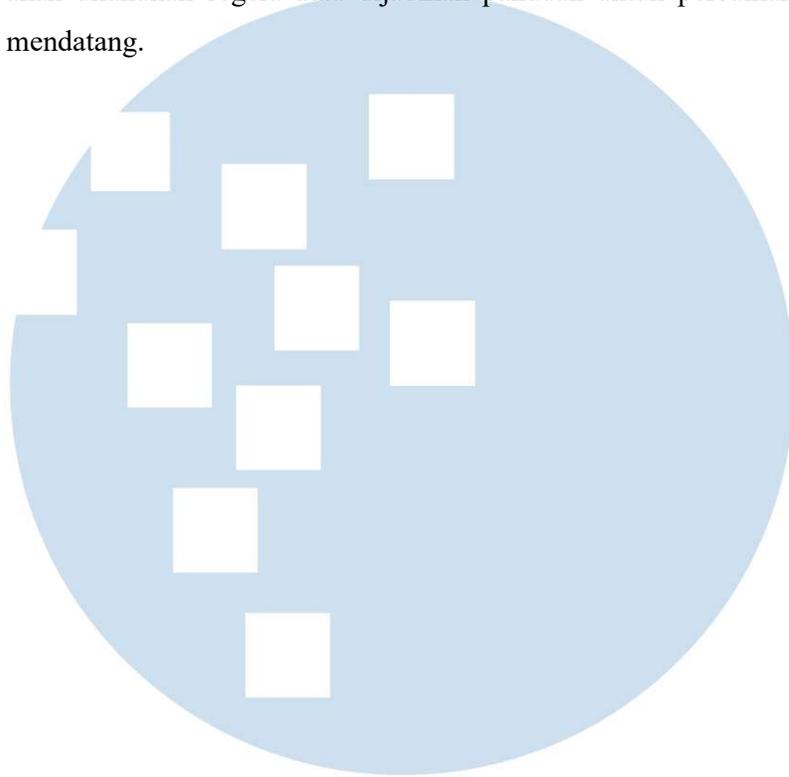
c. Penyusunan Laporan (*Reporting*)

Setelah proses pengumpulan data, informasi yang diperoleh akan diproses dan dihitung untuk menentukan tingkat kematangan (*maturity level*). Pada tahap ini, laporan audit akan disusun untuk memberikan informasi mengenai hasil audit. Perhitungan maturity level didasarkan pada hasil wawancara, survei, dan rekapitulasi kuesioner. Dengan memperhitungkan maturity level saat ini dan standar kinerja ideal, dilakukan analisis untuk mengidentifikasi kesenjangan (*gap*) dan penyebabnya.

d. Tindak Lanjut (*Follow Up*)

Tahap ini melibatkan penyampaian rekomendasi perbaikan kepada manajemen objek yang diaudit. Keputusan untuk menerapkan rekomendasi

perbaikan menjadi tanggung jawab manajemen objek yang diaudit, apakah akan dilakukan segera atau dijadikan panduan untuk perbaikan di masa mendatang.



UMMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA