Jurnal Teknik Informatika dan Teknologi Informasi
Volume. 5 Nomor. 2 Agustus 2025
E-ISSN: 2827-9387, P- ISSN: 2827-9379, Hal 237-262
DOI: https://doi.org/10.55606/jutiti.v5i2.5557
Available Online at : https://journalshub.org/index.php/jutiti

Evaluasi Website E-Wartawan Menggunakan ISO 27001 dalam Meningkatkan Keamanan Informasi di Kantor Diskominfotik

Rapiana[1*], Mansur [2]
[1-2] Jurusan Teknik Informatika, Program Studi Keamanan sistem informasi, Politeknik Negeri Bengkalis, Indonesia
finaf9859@gmail.com[1], Mansur@polbeng.ac.id [2]

Alamat: Jl. Bathin Alam, Sungai Alam, Bengkalis - Riau 28712
*Korespondensi penulis: finaf9859@gmail.com**

Abstract. *Information security is a crucial aspect in managing digital government systems, particularly for services that store sensitive data. The e-Journalist website managed by the Bengkalis Regency Communications and Information Technology Office Discominfotik serves as a communication medium between the government and the press, requiring optimal information security to prevent data leaks or misuse. This study aims to evaluate the level of information security in the e-Journalist system using the ISO/IEC 27001 standard. The evaluation was conducted based on the seven main clauses of ISO 27001: Organizational Context, Leadership, Planning, Support, Operation, Evaluation, and Improvement, and used the SSE-CMM maturity level measurement approach. The research method used was a quantitative approach through questionnaire distribution and direct observation. The evaluation results showed an average maturity level score of 2.39, which falls into the Repeatable but Intuitive category, meaning that information security processes have been implemented repeatedly but have not been formally documented.*

Keywords: *information security, ISO 27001, Maturity level,Diskomingotik, E-Wartawan*

Abstrak.:Keamanan informasi merupakan aspek yang sangat penting dalam pengelolaan sistem digital pemerintahan, terutama pada layanan yang menyimpan data sensitif. Website e-Wartawan yang dikelola oleh Kantor Diskominfotik Kabupaten Bengkalis berfungsi sebagai media komunikasi antara pemerintah dan insan pers, sehingga memerlukan pengamanan informasi yang optimal bagi mencegah terjadinya kebocoran atau penyalahgunaan data. Penelitian ini bertujuan bagi mengevaluasi tingkat keamanan informasi pada sistem e-wartawan dengan mengacu pada standar ISO/IEC 27001. Evaluasi dilakukan berdasarkan tujuh klausul utama ISO 27001, yaitu Konteks Organisasi, Kepemimpinan, Perencanaan, Dukungan, Operasi, Evaluasi, dan Perbaikan, serta menggunakan pengukuran tingkat kematangan maturity level dengan pendekatan SSE-CMM. Metode penelitian yang digunakan yakni pendekatan kuantitatif melalui penyebaran kuesioner dan observasi langsung. Hasil evaluasi menunjukkan bahwa skor rata-rata tingkat kematangan berada pada angka **2,39**, yang termasuk dalam kategori ***Repeatable but Intuitive***, yaitu proses keamanan informasi telah dilaksanakan secara berulang namun belum terdokumentasi secara formal.

Kata kunci: Keamanan informasi, ISO/IEC 27001, Maturity level

1. LATAR BELAKANG

Informasi telah menjadi aset yang sangat berharga dan krusial bagi keberlanjutan suatu organisasi di lingkungan digital yang berkembang pesat saat ini. Oleh karena itu, kerusakan atau pelanggaran informasi dapat berdampak negatif bagi organisasi. Kekhawatiran akan keamanan informasi semakin meningkat seiring dengan kebutuhan akan informasi. Bagi perusahaan, organisasi, dan pemerintah, kerentanan informasi yang semakin meningkat menimbulkan tantangan yang lebih rumit terhadap keamanan informasi [1]. Bagi memastikan tingkat kematangan dan kelengkapan keamanan informasi kantor Diskominfotik, diperlukan evaluasi. Indeks Keamanan Informasi (KAMI) Kementerian Komunikasi dan Informatika yang

Received: Juni 14, 2025; Revised: Juni 28, 2025; Accepted: Juli 10, 2025; Online Available: Juli 12, 2025

telah memenuhi standar dan aspek keamanan informasi sebagaimana dimaksud dalam ISO 27001 digunakan bagi penilaian.[2].

ISO 27001:2022 yakni standar yang diterbitkan oleh Organisasi Internasional bagi Standardisasi. Standar ini berfungsi sebagai panduan bagi membantu bisnis menjaga keamanan aset dan sistem manajemen keamanan informasi mereka tetap mutakhir. Standar ini dirancang khusus bagi memenuhi kebutuhan dalam menciptakan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi[3].

Kantor Diskominfotik Kabupaten Bengkalis mengelola data teknologi informasi dan komunikasi (TIK) yang mencakup berbagai aspek penting. Ini meliputi data infrastruktur TIK seperti yang terdapat dalam data e-wartawan, serta pemanfaatan teknologi digital di berbagai sektor. Selain itu, mereka juga memantau data penggunaan aplikasi dan platform digital oleh masyarakat, termasuk tren media sosial*, e-commerce,* dan layanan publik online. Data ini memberikan gambaran menyeluruh tentang perkembangan TIK di bengkalis, membantu mengidentifikasi kebutuhan dan peluang pengembangan, serta mendukung pengambilan keputusan yang tepat bagi meningkatkan akses dan kualitas layanan TIK bagi masyarakat.

Pada penelitian tersebut keamanan informasi yang diukur pada kantor Diskominfotik berdasarkan standar ISO 27001 yaitu: Konteks organisasi (klausul 4), Kepemimpinan (klausul 5), Perencanaan (klausul 6), Dukungan (klausul 7), Operasi (klausul 8), Evaluasi (klausul 9), Perbaikan (klausul 10).

Menerapkan standar keamanan informasi yang diterima secara global sangat penting bagi mencapai tingkat keamanan informasi yang tinggi. ISO 27001:2022 yakni salah satu standar yang telah terbukti efektif. Standar ini menawarkan kerangka kerja yang komprehensif bagi menciptakan, menerapkan, menjalankan, memantau, mengevaluasi, memelihara, dan meningkatkan sistem manajemen keamanan informasi.

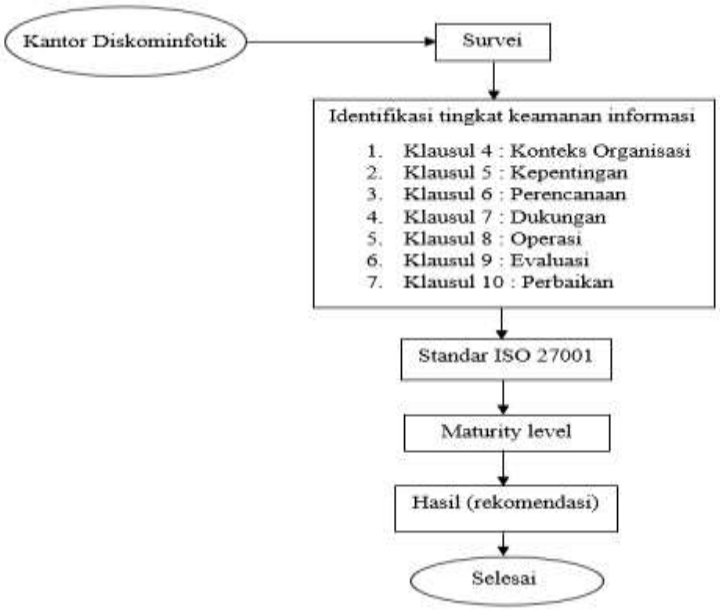
2. KAJIAN TEORITIS

ISO/IEC 27001 merupakan standar yang umum digunakan bagi mengimplementasikan keamanan sistem informasi. Penerapan standar ini melindungi aspek kerahasiaan, integritas, dan ketersediaan informasi. Dalam konteks tata kelola pemerintahan, keamanan data dan Bagi mencapai tata kelola yang baik dan bersih, informasi sangatlah penting. Kemampuan bagi menyampaikan informasi dengan cepat dan tepat sangatlah penting. Bagi memastikan bahwa kontrol keamanan informasi memenuhi standar, ISO/IEC 27001 yakni kerangka kerja yang memberikan instruksi tentang cara membangun sistem manajemen keamanan informasi dan sertifikasi global. Struktur organisasi, peran, perencanaan, kebijakan, prosedur, praktik, dan

sumber daya yang lengkap semuanya tercakup dalam sistem manajemen keamanan informasi. [5].

Model kematangan (tingkat kematangan) merupakan salah satu instrumen yang digunakan bagi mengukur kinerja keamanan informasi. Model kematangan ini merupakan metode bagi mengevaluasi seberapa baik manajemen dalam mengadopsi keamanan informasi dengan melihat perkembangan proses manajemen. Proses sistem informasi dapat dikelola dan dikendalikan menggunakan model kematangan yang berkisar dari level 0 (tidak ada) hingga level 5 (optimis), yang didasarkan pada teknik evaluasi organisasi. Tujuan dari model kematangan ini yakni memprioritaskan perbaikan dan mengidentifikasi permasalahan terkini. Perusahaan dapat mengidentifikasi model kematangan sebagai representasi potensi kondisi saat ini dan di masa mendatang karena model ini dimaksudkan bagi berfungsi sebagai profil proses keamanan informasi. Model ini memanfaatkan model kematangan yang ditetapkan ISO 27001 bagi setiap pengendalian. memungkinkan manajemen bagi menentukan keadaan perusahaan saat ini, keadaan industri saat ini bagi perbandingan, keadaan yang dituju perusahaan, dan pertumbuhan yang direncanakan.

3. METODE PENELITIAN



Gambar 1. Tahapan Survei

- Survei

  Tahap ini melibatkan pengumpulan data seperti data media perusahaan, data pribadi wartawan, data berita. Data tersebut sangat penting bagi dievaluasi menggunakan ISO 27001, bagi memastikan keamanan, integritas dan ketersediaan data. Terkait keamanan

informasi melalui wawancara atau observasi langsung ke kantor Diskominfotik. Tujuan survei yaitu bagi mendapatkan pemahaman menyeluruh tentang keamanan informasi yang ada di kantor Diskominfotik.

- Identifikasi tingkat keamanan

  Setelah mengumpulkan data melalui survei, selanjutnya yaitu mengidentifikasi tingkat keamanan yang ada pada kantor Diskominfotik. Identifikasi ini yaitu bagi mengukur sejauh mana organisasi dalam menjaga kerahasiaan, integritas dan ketersediaan informasi. Tahap ini sangat penting agar dapat memberikan suatu gambaran yang jelas tentang kondisi keamanan informasi saat ini [13].

  Pada penelitian ini keamanan informasi yang diukur pada kantor Diskominfotik peneliti menggunakan 7 klausul yakni sebagai berikut:

  a. Klausul 4 : Konteks Organisasi
  b. Klausul 5 : Kepemimpinan
  c. Klausul 6 : Perencanaan
  d. Klausul 7 : Dukungan
  e. Klausul 8 : Operasi
  f. Klausul 9 : Evaluasi
  g. Klausul 10 : Perbaikan

- Standar ISO 27001

  Setelah mengetahui tingkat keamanan informasi yang ada di kantor Diskominfotik, langkah selanjutnya yakni membandingkan hasil tersebut dengan standar ISO 27001. Langkah ini bertujuan bagi menilai sejauh mana kantor tersebut telah memenuhi standar keamanan informasi yang diakui sebagai aturan atau pedoman yang telah disepakati oleh banyak negara di seluruh dunia bagi memastikan keamanan, dan cara kerja yang baik dalam suatu bidang. Dalam hal ini, standar internasional seperti ISO 27001. Penelitian ini mengacu pada beberapa klausul dalam ISO 27001, di mana setiap klausal memiliki pertanyaan yang sesuai dengan standar tersebut.

- Selesai

  Setelah melakukan perbandingan terhadap standar ISO 27001, selanjutnya yaitu mengevaluasi *maturity level* keamanan informasi di kantor Diskominfotik. *Maturity level* ini mengacu pada tingkat keamanan atau kematangan suatu sistem informasi dalam suatu organisasi. Tujuan *maturity level* ini yakni bagi mengukur sejauh mana praktek terbaik yang direkomendasikan oleh standar ISO 27001 tersebut. *Maturity level*

ini juga diukur dengan menggunakan kerangka kerja yang menggambarkan tahap perkembangan dari awal level 1 hingga tingkat kematangan yang tinggi level 5. *Indeks Maturity* yang didapat kemudian dibuat ke dalam skala yang akan dipetakan lagi ke dalam *maturity level* bagi mengetahui tingkat kematangannya.

Level Capability SSE-CMM (Systems Security Engineering Capability Maturity Model) yakni sebuah kerangka kerja yang digunakan bagi mengevaluasi dan meningkatkan kemampuan organisasi dalam bidang rekayasa keamanan sistem (system security engineering). SSE-CMM mengukur seberapa baik organisasi mengelola dan menerapkan proses keamanan dalam siklus hidup sistem informasi mereka. SSE-CMM terdiri dari dua bagian, yaitu :

Model bagi teknik keamanan proses, proyek dan organisasi

Model ini menjelaskan cara suatu organisasi dapat secara terstruktur dan teratur dalam mengelola dan menerapkan keamanan informasi. Tujuannya yakni bagi memastikan bahwa perlindungan informasi diterapkan dengan baik di setiap tahap, mulai dari pelaksanaan proyek hingga kegiatan rutin sehari-hari dalam organisasi.

Metode penilaian bagi mengetahui proses kematangan

Metode penilaian ini digunakan bagi menilai seberapa baik suatu organisasi menerapkan keamanan informasi secara efektif dan berkelanjutan. Penilaian ini juga membantu mengetahui sejauh mana kemajuan organisasi dalam menjaga keamanan informasi serta memberikan panduan Langkah-langkah yang dapat diambil bagi perbaikan dan peningkatan keamanan.

Model ini memberikan panduan bagi meningkatkan proses rekayasa sistem keamanan, sehingga organisasi dapat memastikan bahwa mereka melindungi aset informasi dan memenuhi standar keamanan yang diinginkan. Dapat disimpulkan bahwa CMM yakni suatu model yang digunakan bagi mengukur kematangan proses pembuatan perangkat lunak dalam sebuah organisasi dan memberikan pedoman bagi meningkatkan ke level selanjutnya.

Bagi memastikan tingkat kapasitas setiap area proses, evaluasi perlu dilakukan. Hal ini menunjukkan bahwa area proses yang berbeda dapat dan kemungkinan besar akan memiliki kapasitas yang berbeda-beda. Informasi ini kemudian dapat digunakan oleh perusahaan bagi menargetkan peningkatan prosesnya. Tujuan bisnis organisasi perlu dipertimbangkan saat menentukan prioritas dan urutan tindakan bagi peningkatan proses. *Level Capability SSE-CMM (System Security Engineering Capability Maturity Model*) memiliki 5 tingkat dalam SSE-CMM yaitu. *Level 1 "Initial / Ad Hoc", Level 2 "Repeatable But Intuitive", Level 3*

"Defined Process", Level 4 Managed And Measurable", Level 5 "Optimized". Masing-masing level akan dijelaskan sebagai berikut:

- *Initial*

  Pada level ini, proses pembuatan perangkat lunak digambarkan sebagai proses yang tidak teratur dan seringkali kacau. Organisasi biasanya tidak menyediakan lingkungan yang stabil bagi mengembangkan produk baru. Organisasi yang berada di level ini mungkin mempunyai prosedur formal bagi perencanaan dan penelusuran kerja mereka tetapi tidak ada mekanisme manajemen bagi memastikan bahwa prosedur tersebut digunakan dalam kerja mereka. Satu alasan utama mengapa suatu organisasi bekerja dengan cara itu yakni karena mereka belum pernah menerima keuntungan dari sebuah proses yang matang sehingga organisasi tersebut tidak mengenai konsekuensi dari tindakan mereka yang kacau.

- *Repeatable*

  Level ini memiliki kelebihan yang tidak dimiliki level Initial, yaitu mengadakan kontrol terhadap cara organisasi dalam membuat rencana dan komitmennya. Organisasi melakukan kontrol dengan belajar membuat serta memenuhi perkiraan dan rencana mereka. Pada level ini, proses manajemen proyek yang dasar telah digunakan bagi melakukan pengawasan biaya, jadwal, komitmen, dan perubahan. Selain itu, juga terdapat proses-proses yang diperlukan bagi mengulangi keberhasilan proyek dengan aplikasi yang sama.

- *Defined*

  Pada level Defined, organisasi telah memiliki dasar unak perkembangan yang terus-menerus. Misalnya, ketika tim pembuat perangkat lunak menghadapi sebuah masalah, mereka akan cenderung menggunakan proses yang telah didefinisikan. Dasar tersebut telah dibuat bagi memeriksa proses dan memutuskan bagaimana memperbaiki proses tersebut. Organisasi mendefinisikan proses sebagai dasar bagi implementasi yang konsisten dan mudah dimengerti. Proses pembuatan perangkat lunakdistandarisasi, didokumentasikan, dan dimasukkan ke dalam proses pengembangan perangkat lunak standar perusahaan bagi tugas-tugas teknik dan manajemen. Prosedur normal bagi membuat item baru dicatat pada tahap ini. Fondasi dari prosedur ini yakni pengembangan produk yang terintegrasi. Manajer, pemimpin tim, dan anggota tim pengembangan dapat bertindak lebih efektif dengan bantuan proses ini. Program pelatihan organisasi diterapkan bagi memastikan manajer dan

karyawan memiliki pengetahuan bagi melaksanakan tanggung jawab mereka. Tanggung jawab dan tugas didefinisikan dan dipahami dengan baik. Berkat definisi proses pengembangan perangkat lunak yang jelas, manajemen memiliki pandangan yang baik tentang perkembangan teknis dalam semua proyek. Biaya, jadwal, dan kebutuhan proyek dikontrol dan kualitas produk dijaga.

- *Managed*

  Pada level Managed, organisasi telah memulai pengukuran dan analisis proses yang lengkap. Ada pengumpulan hasil pengukuran detail dari proses pembuatan perangkat lunak dan kualitas produk yang telah dimengerti secara kualitatif dan terkendali. Seluruh organisasi terfokus pada perbaikan proses yang terus-menerus. Proyek dikontrol dalam hal produk dan prosesnya dengan menjelaskan variasi pada kinerja mereka terhadap batas-batas yang masih bisa diterima. Proses pengembangan dapat diperkirakan karena proses diukur dan dioperasikan dalam batasan pengukuran.

- *Optimized*

  Pada level ini manajer pengembangan perangkat lunak memfokuskan pada produk mereka dan secara khusus akan mengumpulkan serta menganalisis hanya pada data yang secara langsung berhubungan dengan perbaikan produk. Dengan proses optimisasi, organisasi mempunyai alat bagi mengidentifikasi elemen-elemen yang lemah dari proses dan memperbaikinya. Organisasi memiîiki media bagi mengidentifikasikan kekurangan dan kelebihan proses dengan tujuan mencegah terjadinya kesalahan. Tim pengembangan produk menganalisis kegagalan dan kesalahan bagi menemukan penyebabnya. Proses pengembangan dievaluasi bagi mencegah kegagalan dan kesalahan yang telah diketahui terulang kembali serta pelajaran yang diperoleh digunakan pada proyek yang lain. Perbaikan terjadi karena peningkatan pada proses yang ada dan dengan inovasi yang menggunakan teknologi dan metode baru. Perbaikan proses yang terus-menerus dimungkinkan oleh adanya umpan balik yang kuantitatif dari proses dan pengendalian ide-ide serta teknologi yang inovatif.

  Perhitungan tingkat kematangan: Rata-rata semua pengendalian keamanan yang tingkat kapabilitasnya telah ditentukan menghasilkan nilai tingkat kematangan. Setiap klausa mencakup beberapa tujuan pengendalian, dan setiap tujuan pengendalian memiliki beberapa pengendalian keamanan informasi. Nilai tingkat kematangan bagi setiap tujuan pengendalian dihitung dengan merata-ratakan pengendalian keamanan

informasi. Sementara itu, rata-rata tujuan pengendalian yang digunakan dalam setiap kalimat digunakan bagi menentukan nilai tingkat kematangan bagi klausa tersebut. Perbedaan antara tingkat kematangan dan nilai kematangan disorot dalam studi ini. Proses mencapai tingkat kapasitas tertentu dapat menghasilkan nilai kematangan non-integer (desimal). Sedangkan tingkat kematangan lebih menunjukkan tahapan atau kelas yang dicapai dalam proses kapabilitas yang dinyatakan dalam bilangan bulat. Skala *indeks maturity* dan *maturity level* ditunjukkan pada tabel :

Tabel 1. Maturity Level

Maturity Index	**Maturity Level**
0 – 0.49	0 – Non Existent
0.50 – 1.49	1 – Initial/Ad hoc
1.50 – 2.49	2 – Repeatable But Intuitive
2.50 – 3.49	3 – Defined Process
3.50 – 4.49	4 – Managed and Measurable
4.50 – 5.00	5- Optimized

Tabel 2. Deskripsi Maturity Level

Level	**Deskripsi**
0 - Non Existent	Belum adanya permasalahan yang harus diatasi. Perusahaan merasa tidak membutuhkan mekanisme proses keamanan. Sehingga tidak ada pengawasan sama sekali.
1 - *Initial/ Ad Hoc*	Sudah adanya bukti bahwa perusahaan mengetahui adanya permasalahan yang harus diatasi. Perusahaan sudah memiliki inisiatif bagi melakukan keamanan. Namun sifatnya masih non formal.
2 - *Repeatable but Intuitive*	Sudah adanya perencanaan, pengelolaan, dan implementasi sistem berbasis komputer yang lebih terarah. Perusahaan memiliki kebiasaan terpola bagi merencanakan keamanan yang dilakukan secara berulang namun belum melibatkan dokumentasi formal.
3 – *Defined Process*	Sudah memiliki proses keamanan yang sudah didokumentasikan dengan baik kemudian dikomunikasikan melalui pelatihan. Perusahaan juga menyadari perlunya proses keamanan sehingga adanya aturan yang menunjukkan bagi perusahaan secara rutin melakukan keamanan.
4 – *Managed and Measurable*	Sudah adanya proses komputerisasi dengan baik, pengembangan sistem sudah terarah dan dijalankan secara terorganisir. Proses keamanan sudah secara formal dilakukan dan secara terus menerus dievaluasi bagi meningkatkan layanan perusahaan.

5 - *Optimized*	Sudah mengikuti best practice yang ditandai dengan adanya proses otomatisasi pada sistem dengan metodologi yang tepat.

Index maturity level atau tingkat kematangan yakni pengukuran yang digunakan bagi mengetahui sejauh mana proses manajemen teknologi informasi (TI) dalam sebuah perusahaan telah dikelola dengan baik.

Bagi mengetahui tingkat kematangan (*Maturity Level*) Klausul dan Annex menggunakan rumus *maturity level*.

$$\text{Index Maturity} = \frac{\textit{Jumlah pertanyaan yang dijawab}}{\textit{Jumlah pertanyaan klausan dan annex}} * 100$$

Pada rumus di atas menjelaskan bagaimana cara mengetahui tingkat kematangan Klausul dan Annex, yaitu dengan cara menjumlahkan skor pertanyaan yang dijawab oleh responden kemudian dibagi dengan total pertanyaan klausul dan annex lalu dikalikan dengan 100%. Dengan mengikuti langkah-langkah ini kantor Diskominfotik dapat meningkatkan perlindungan terhadap data yang dimiliki dan memenuhi standar ISO 27001, bagi mencapai tingkat *maturity level* yang lebih tinggi, serta menghadapi ancaman yang ada.

Rekomendasi Perbaikan

Berdasarkan hasil dari evaluasi keamanan informasi dan *maturity level* diatas, tahap terakhir yaitu menyusun hasil rekomendasi. Yang berfungsi bagi memberikan masukan serta tindakan yang perlu dilakukan bagi memperbaiki keamanan informasi. Rekomendasi ini meningkatkan kesadaran bagi pengguna, serta bagi meningkatkan tingkat keamanan informasi pada kantor Diskominfotik bengkalis.

Berikut penelitian ini melampirkan beberapa pertanyaan terkait 7 klausul yang akan digunakan.

Klausul 4: Konteks organisasi

Menganalisis kebutuhan dan ekspektasi pemangku kepentingan serta mendefinisikan parameter sistem manajemen keamanan informasi merupakan tujuan utama Klausul 4 ISO 27001. Organisasi harus memahami dan menilai elemen internal dan eksternal yang mungkin

berdampak pada ISMS agar dapat mematuhi paragraf ini. Paragraf ini menjamin bahwa sistem manajemen dirancang bagi memenuhi persyaratan dan ekspektasi spesifik para pemangku kepentingan sekaligus mengatasi risiko yang relevan dengan lingkungan organisasi dengan menetapkan batasan sistem yang sesuai.

Tabel 3. Klausul 4: Konteks organisasi

Item Pertanyaan	Jawaban	Pembuktian	Skor	Maturity
Apakah kebijakan telah disetujui oleh atasan langsung?	disetujui	Persetujuan ini menjadi Langkah penting bagi memastikan kebijakan keamanan informasi berjalan sesuai dengan rencana dan dapat diterapkan oleh seluruh pihak terkait.	3	*Defined*
Apakah kebijakan keamanan informasi telah di sosialisasikan?	Sudah	Ketika sebuah program itu mau di launching yang pertama bikin sop. kebijakan keamanan informasi disosialisasikan agar wartawan dan pegawai memahami cara melindungi data penting. seperti data ktp dan data notaris.	3	*Defined*
Apakah kebijakan mencakup perlindungan terhadap e-wartawan?	Mencangkup		3	*Defined*
Apakah kebijakan diterima oleh pihak lain yang relevan?	Sudah	Karena bagi memastikan mereka memahami dan menerima isi dari kebijakan.	3	*Defined*
Apakah kebijakan keamanan informasi tersebut sudah melalui proses peninjauan dan evaluasi secara berkala?	Sudah	Evaluasinya dalam bentuk penambahan fitur pengajuan proposal kerjasama via online, jadi seluruh persyaratan dibuat pdf, dan upload nanti di verifikasi dalam setiap tahun.	3	*Managed and measurable*
Apakah kebijakan tersebut sudah dipublikasikan?	Sudah	Perbup no 86 tahun 2017 dan sudah disosialisasikan.	3	*Defined*

Apakah terdapat jadwal yang jelas bagi pelaksanaan tinjauan ulang kebijakan keamanan informasi website e-wartawan?	Sudah	Jadwal sesuai kondisi, ketika ada keluhan atau permintaan baru dikerjakan atau ditangani langsung.	3	*Managed and measurable*
Apakah kebijakan yang diterapkan sesuai dengan aturan yang telah berlaku?	Sudah	Perbup no 86 thn 2017	3	*Managed and measurable*
Apakah sudah ada kebijakan keamanan informasi?	Ada		3	*Defined*
Score Maturity			**3**	

Sumber : Data Penelitian lapangan (2024)

Berdasarkan hasil pengumpulan data melalui kuesioner dan wawancara terhadap implementasi sub klausul konteks organisasi, pada sistem informasi e-wartawan, dapat kita ketahui bahwa jumlah keseluruhan keamanan informasi memiliki maturity indeks sejumlah 3 berikut rumus bagi mencari score maturity nya

$$\text{Indeks Maturity} = \frac{27}{9} * 100\%$$

Hasil penjumlahan bagi score pertanyaan yang dijawab dengan 27 kemudian dibagi dengan 9 dengan banyaknya jumlah pertanyaan klausul maka dapatlah hasilnya 3 kemudian di kali 100% bagi mengalikan hasil pembagian dengan 100% cukup mengalikan hasil pembagian dengan 1 atau 100* dalam bentuk desimal yaitu 1. Langkah ini tidak akan mengubah nilai dari hasil pembagian sebelumnya, karena mengalikan dengan satu akan mendapatkan nilai yang sama.

Klausul 5: Kepemimpinan

Tugas dan tanggung jawab manajemen puncak dalam menerapkan sistem manajemen keamanan informasi digarisbawahi dalam Klausul 5 ISO 27001. Ketentuan ini mewajibkan manajemen puncak bagi secara aktif mendukung dan membimbing implementasi ISMS, termasuk menetapkan tujuan, mengalokasikan sumber daya, dan menyusun kebijakan. Bagi memastikan bahwa sistem manajemen diterapkan secara berkala dan mendapatkan dukungan yang dibutuhkan bagi mencapai hasil yang diinginkan, kepemimpinan yang efektif dan komitmen manajemen sangat penting.

Tabel 4. Klausul 5: Kepemimpinan

Item Pertanyaan	Jawaban	Pembuktian	Skor	Maturity
Apakah semua pegawai yang terlibat dalam pengelolaan data e-wartawan telah diberikan pelatihan keamanan informasi secara berkala?	Sudah		3	*Defined*
Apakah semua perangkat lunak yang digunakan oleh e-wartawan telah digunakan dengan sah?	Sah		3	*Defined*
Apakah ada prosedur bagi melapor jika terjadi kehilangan atau kerusakan perangkat?	Ada	Mooring, atau sistem pengaturan yang memungkinkan perangkat lunak software tetap terkoneksi meskipun terjadi gangguan. jadi, ketika software down cukup mengganti alamat Ip nya saja. setelah ip diubah, sistem akan otomatis kembali aktif dan berjalan seperti biasa tanpa perlu konfigurasi ulang.	3	*Defined*

Apakah ada prosedur bagi memusnahkan data yang sudah tidak diperlukan lagi (misalnya, draft berita yang sudah dipublikasikan?	Ada	Dinas perpustakaan dan arsip daerah, jika mereka meminta data ke Diskominfo, mereka harus mengajukan permintaan secara resmi melalui surat, surat tersebut berisi permintaan penyerahan arsip atau data yang sudah tidak digunakan lagi.	3	*Managed and measurable*
Apakah wartawan diberikan pelatihan tentang cara merawat perangkat dan menjaga kerahasiaan data?	Ada	Dengan cara penggunaan perangkat dengan benar, pengaturan keamanan perangkat, pembaruan perangkat lunak dan penggunaan antivirus.	3	*Defined*
Siapa yang bertanggung jawab bagi melakukan penyelidikan ketika terjadi insiden keamanan, seperti kebocoran data?	Kabid sdki	Prarezeki Indra muda	3	*Defined*
Score Maturity	**3**			

Sumber : Data Penelitian lapangan (2024)

Berdasarkan hasil pengumpulan data melalui kuesioner dan wawancara terhadap implementasi sub klausul kepemimpinan, pada sistem informasi e-wartawan dapat kita diketahui bahwa jumlah keseluruhan keamanan memiliki indeks maturity level 3,1 berikut rumus bagi mencari score maturity

$$\text{Indeks Maturity} = \frac{18}{6} * 100\%$$

Hasil penjumlahan bagi score pertanyaan yang dijawab dengan 19 kemudian dibagi dengan 6 dengan banyaknya jumlah pertanyaan klausul maka dapatlah hasilnya 3 kemudian di kali 100% bagi mengalikan hasil pembagian dengan 100% cukup mengalikan hasil pembagian dengan 1 atau 100* dalam bentuk desimal yaitu 1. Langkah ini tidak akan mengubah nilai dari hasil pembagian sebelumnya, karena mengalikan dengan satu akan mendapatkan nilai yang sama.

Klausul 6: Perencanaan

Menetapkan tujuan keamanan informasi dan mengevaluasi peluang serta risiko tercakup dalam Klausul 6 ISO 27001. Ketentuan ini menjamin bahwa perusahaan menetapkan tujuan keamanan informasi yang spesifik dan mengenali serta mengendalikan risiko dan peluang yang dapat membahayakan pencapaian tujuan tersebut.

Tabel 5. Klausul 6 Perencanaan

Item Pertanyaan	Jawaban	Pembuktian	Skor	Maturity
Apakah terdapat kebijakan bagi prosedur terkait tindakan bagi menangani resiko keamanan informasi?	Belum	Belum ditemukan adanya kebijakan formal atau prosedur terdokumentasi yang mengatur secara khusus tentang penanganan risiko keamanan informasi.	1	*Initial*
Apakah ada dokumentasi SOP yang mengatur standar pelayanan e-wartawan?	Ada, dalam bentuk SOP teknis		3	*Defined*
Apakah ada prosedur pemulihan data yang jelas jika terjadi kehilangan data?	Ada backup		3	*Defined*
Apakah aset informasi tersebut telah diberi label berdasarkan tingkat kerahasiaan?	Belum	Karena belum ada shaf yang ditempel. Dengan arti belum ada label atau simbol yang diberikan pada aset informasi tersebut.	1	*Initial*
Apakah ada prosedur bagi membackup data secara teratur?	Ada yang otomatis dan manual		3	*Defined*

Apakah ada mekanisme bagi melacak perubahan pada aset informasi dan memastikan bahwa perubahan tersebut didokumentasikan dengan baik?	Ada	Dengan adanya log, organisasi memiliki mekanisme bagi memantau, melacak dan mendokumentasikan semua perubahan pada aset informasi, yang merupakan bagian penting.	3	*Defined*
Bagaimana kantor kominfotik memastikan perlindungan data pribadi wartawan sesuai dengan regulasi perlindungan data yang berlaku?	Ada	Dengan website e-wartawan data privat perusahaan aman terdokumentasi dasarnya perbup 86 tahun 2017 sebagai dasar hukumnya.	3	*Defined*
Apakah asetnya informasi yang bersifat rahasia disimpan di tempat yang aman dan dilindungi dengan akses yang terbatas?	Aman dan terbatas	Asetnya tersimpan di ruangan server. Ada dua bentuk asset informasinya. 1. aplikasi e-wartawan 2. SPJ administrasinya	3	*Defined*
Score Maturity			**2,5**	

Sumber : Data Penelitian lapangan (2024)

Berdasarkan hasil pengumpulan data melalui kuesioner dan wawancara terhadap implementasi sub klausul perencanaan, pada sistem informasi e-wartawan, dapat kita ketahui bahwa jumlah keseluruhan keamanan informasi memiliki maturity indeks sejumlah 2,5 berikut rumus bagi mencari score maturitasnya

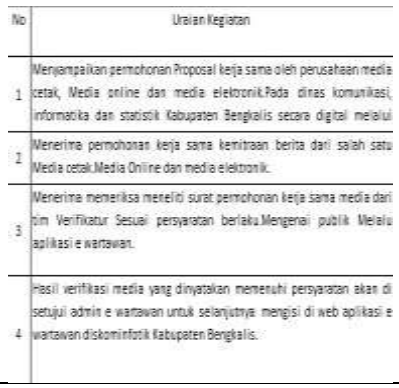
$$\text{Indeks Maturity} = \frac{20}{8} * 100\%$$

Hasil penjumlahan bagi score pertanyaan yang dijawab dengan 20 kemudian dibagi dengan 8 dengan banyaknya jumlah pertanyaan klausul maka dapatlah hasilnya 2,5 kemudian di kali 100% bagi mengalikan hasil pembagian dengan 100% cukup mengalikan hasil pembagian dengan 1 atau 100* dalam bentuk desimal yaitu 1. Langkah ini tidak akan mengubah nilai dari hasil pembagian sebelumnya, karena mengalikan dengan satu akan mendapatkan nilai yang sama.

Klausul 7: Dukungan

Sumber daya yang dibutuhkan bagi menerapkan ISMS, beserta pengetahuan, keterampilan, dan komunikasi yang dibutuhkan, tercakup dalam Klausul 7 ISO 27001. Bagi mendukung operasional ISMS, klausul ini memastikan bahwa organisasi menyediakan sumber daya yang memadai, melatih individu yang terlibat, meningkatkan kesadaran akan pentingnya keamanan informasi, dan menjaga komunikasi yang baik.

Tabel 6. Klausul 7: Dukungan

Item Pertanyaan	Jawaban	Pembuktian	Skor	Maturity
Apakah akses ke data e-wartawan dibatasi?	Iya	Dibatasi, kalau bagi cpanel, server, sistem hanya pengguna website e-wartawan saja. Tapi kalau bagi admin ke web mulai dari kabib kemudian staf.	3	*Defined*
Apakah ada mekanisme bagi memantau aktivitas akses terhadap data e-wartawan dan mendeteksi adanya akses yang tidak sah?	Ada		3	*Defined*
Bagaimana kominfotik memastikan bahwa hak akses pegawai terhadap data e-wartawan sesuai dengan tugas dan tanggung jawab masing-masing?	Diberi tugas masing-masing	Dengan memastikan sesuai instruksi dari pimpinan saja. Contoh ketika ingin membuat SPJ (surat penanggung jawaban). Maka harus memastikan bahwa website itu harus tetap normal berarti kami akan mengecek secara berkala.	3	*Defined*
Apakah wartawan diberikan pelatihan secara berkala tentang pentingnya keamanan informasi dan cara menjaga kerahasiaan data?	Belum	Artinya masih otodidak, juga kadang bergabung dengan kawan-kawan programmer dengan mendapatkan pengetahuan dari pengalaman.	0	*Non existent*
Apakah ada mekanisme bagi memulihkan akses yang hilang atau terlupakan secara aman?	Ada	Dengan membackup dan diletakkan satu tempat, ada di eksternal dan di kantor. Bahkan disimpan juga dalam bentuk clouding atau penyimpanan seperti google drive.	3	*Defined*
Apakah organisasi menyimpan bukti atau log pelatihan keamanan informasi yang pernah dilakukan?	Belum	Karena belum adanya pencatatan formal terkait pelatihan keamanan informasi.	0	

Score Maturity	**2**

Sumber : Data Penelitian lapangan (2024)

Berdasarkan hasil pengumpulan data melalui kuesioner dan wawancara terhadap implementasi sub klausul dukungan, pada sistem informasi dapat diketahui bahwa jumlah keseluruhan keamanan informasi memiliki maturity indeks sejumlah 2 berikut rumus bagi mencari score maturitasnya

$$\text{Indeks Maturity} = \frac{12}{6} * 100\%$$

Hasil penjumlahan bagi skore pertanyaan yang dijawab dengan 12 kemudian dibagi dengan 6 dengan banyaknya jumlah pertanyaan klausul maka dapatlah hasilnya 2 kemudian di kali 100% bagi mengalikan hasil pembagian dengan 100% cukup mengalikan hasil pembagian dengan 1 atau 100* dalam bentuk desimal yaitu 1. Langkah ini tidak akan mengubah nilai dari hasil pembagian sebelumnya, karena mengalikan dengan satu akan mendapatkan nilai yang sama.

Klausul 8: Operasi

Aktivitas dan prosedur yang membentuk sistem manajemen keamanan informasi, seperti manajemen dan pengendalian risiko, dicakup dalam Klausul 8 ISO 27001. Ketentuan ini menjamin bahwa organisasi mengelola risiko yang teridentifikasi, secara konsisten menerapkan prosedur yang ditetapkan bagi mengamankan informasi, dan menggunakan sarana operasional yang efisien bagi menerapkan pengendalian keamanan.

Tabel 7. Klausul 8: Operasi

Item Pertanyaan	Jawaban	perbaikan	Skor	Maturity
Pernahkah komputer ditinggal dalam keadaan menyala?	Pernah		1	*Initial*

Bagaimana kominfo memastikan bahwa peralatan yang digunakan bagi mengelola data e-wartawan dalam kondisi yang baik dan terawat?	Didukung anggaran	Bagi pengelolaan. ada dalam bentuk anggaran yang diberikan. yaitu manajemen web dalam bentuk server, mereka memberikan anggaran. Dengan adanya anggaran yang diberikan oleh pihak kantor maka manfaatkan pihak ketiga bagi melakukan backup secara otomatis.	3	*Defined*
Apakah hasil backup pernah diuji?	Belum	Sampai saat ini belum ada bukti pengujian pemulihan data.	2	*Repeatable but intuitive*
Apakah data e-wartawan disimpan dalam infrastruktur server yang aman secara fisik?	Ya	Data disimpan di ruang server milik diskominfotik yang aksesnya dibatasi.	3	*Defined*
Score Maturity			**2,25**	

Sumber : Data Penelitian lapangan (2024)

Berdasarkan hasil pengumpulan data melalui kuesioner dan wawancara terhadap implementasi sub klausul operasi, pada sistem informasi e-wartawan, diketahui bahwa jumlah keseluruhan keamanan informasi memiliki maturity indeks sejumlah 2,25 berikut rumus bagi mencari score maturitasnya

$$\text{Indeks Maturity} = \frac{9}{4} * 100\%$$

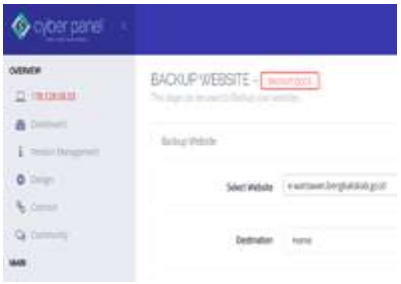
Hasil penjumlahan bagi score pertanyaan yang dijawab dengan 9 kemudian dibagi dengan 4 dengan banyaknya jumlah pertanyaan klausul maka dapatlah hasilnya 2,25 kemudian di kali 100% bagi mengalikan hasil pembagian dengan 100% cukup mengalikan hasil pembagian dengan 1 atau 100* dalam bentuk desimal yaitu 1. Langkah ini tidak akan mengubah nilai dari hasil pembagian sebelumnya, karena mengalikan dengan satu akan mendapatkan nilai yang sama.

Klausul 9: Evaluasi

Kinerja sistem manajemen keamanan informasi dipantau, diukur, dianalisis, dan dievaluasi sesuai dengan Klausul 9 ISO 27001. Ketentuan ini mengamanatkan perusahaan bagi melakukan tinjauan manajemen dan audit internal secara berkala guna memastikan sistem manajemen beroperasi secara efisien, mencapai tujuannya, dan terus berkembang sesuai dengan pengamatan dan masukan.

Tabel 8. Klausul 9: Evaluasi

Item Pertanyaan	Jawaban	Pembuktian	Skor	Maturity
Apakah seluruh karyawan, termasuk wartawan, diberikan tentang cara melaporkan dan menangani insiden keamanan?	Sudah	Tetapi tidak semuanya hanya sebagian karyawan yang diberikan.	2	*Repeatable but intuitive*
Apakah ada pelatihan yang diberikan kepada staf atau karyawan terhadap keamanan e-wartawan?	Tidak	Dengan arti pelatihan itu lebih dari tindak lanjut. Atau proses pengembangan dan peningkatan keterampilan, pengetahuan, dan kesadaran tim dalam menghadapi insiden keamanan informasi. Misalnya bagaimana memperbaiki, bagaimana reaksinya dan lain sebagainya.	0	*Non existent*
Apakah semua karyawan termasuk wartawan, diwajibkan bagi melaporkan setiap insiden keamanan yang mereka temui?	Wajib	Karena dengan melaporkan insiden keamanan setelah ditemukan organisasi dapat mendeteksi potensi ancaman lebih awal. Hal ini memungkinkan tim keamanan bagi merespon dengan cepat sebelum insiden menyebabkan kerusakan lebih besar.	3	*Defined*
Apakah ada pelatihan yang diberikan kepada wartawan tentang cara mengenali dan merespons insiden keamanan?	Ada		3	*Defined*

Apakah ada prosedur bagi merespons insiden keamanan yang melibatkan aset informasi, seperti kebocoran data?	Ada, Wajib	Bahkan prosedur ini tidak dipakai artinya begini kalau prosedur harus dilapor, dari kabib juga lapor ke kadis dan langsung ditindaklanjuti. Karena takut di salah gunakan.	2	*Repeatable buat intuitive*
Apakah semua jenis aset informasi yang digunakan oleh wartawan dilindungi dari kerusakan atau penyalahgunaan?	Belum	Secara klasifikasi cuma dua artinya data umum dan data rahasia. Data umum atau data public ini yakni berita apapun yang dipublikasikan di web Diskominfotik berarti itu berhak bagi dikonsumsi public. Dan yang disebut dengan data rahasia yaitu cuma e-wartawan saja.	0	*Non existent*
Apakah ada mekanisme bagi melindungi aset informasi dari kerusakan, kehilangan, atau penyalahgunaan?	Ada		3	*Defined*
Apakah ada prosedur bagi melakukan audit terhadap aset informasi secara berkala?	Belum	Belum ada.	0	*Non existent*
Apakah ada prosedur bagi melindungi aset informasi dari ancaman internal, seperti kesalahan manusia atau kecurangan?	Belum	Organisasi belum memiliki aturan atau panduan khusus yang dirancang bagi melindungi informasi dari ancaman di dalam, seperti kesalahan staf atau kecurangan. karena belum ada Langkah-langkah yang jelas.	0	*Non existent*

Apakah ada mekanisme bagi mengevaluasi efektivitas Langkah-langkah perlindungan aset informasi?	Ada		3	*Defined*
Score Maturity			**1, 6**	

Sumber : Data Penelitian lapangan (2024)

Berdasarkan hasil pengumpulan data melalui kuesioner dan wawancara terhadap implementasi sub klausul evaluasi, pada sistem informasi dapat diketahui bahwa jumlah keseluruhan keamanan informasi memiliki maturity indeks sejumlah 1,6 berikut rumus bagi mencari score maturitasnya.

$$\text{Indeks Maturity} = \frac{16}{10} * 100\%$$

Hasil penjumlahan bagi score pertanyaan yang dijawab dengan 16 kemudian dibagi dengan 10 dengan banyaknya jumlah pertanyaan klausul maka dapatlah hasilnya 1,6 kemudian di kali 100% bagi mengalikan hasil pembagian dengan 100% cukup mengalikan hasil pembagian dengan 1 atau 100* dalam bentuk desimal yaitu 1. Langkah ini tidak akan mengubah nilai dari hasil pembagian sebelumnya, karena mengalikan dengan satu akan mendapatkan nilai yang sama.

Klausul 10: Perbaikan

Langkah-langkah korektif dan peningkatan berkelanjutan sistem manajemen keamanan informasi tercakup dalam Klausul 10 ISO 27001. Penanganan ketidaksesuaian yang terdeteksi dan penerapan langkah-langkah perbaikan bagi menyelesaikan masalah dan mencegahnya terulang kembali tercakup dalam klausul ini. Tujuannya yakni bagi menjamin bahwa sistem manajemen terus meningkatkan efektivitasnya dengan berkembang dan beradaptasi terhadap perubahan keadaan.

Tabel 9. Klausul 10: Perbaikan

Item Pertanyaan	Jawaban	Pembuktian	Skor	Maturity
Terkait dengan aspek perbaikan berkelanjutan, apa saja aktivitas yang sudah dilakukan oleh organisasi?	Ya	1. Pemeliharaan website secara berkala. 2. Perbaikan fitur saat terjadi gangguan.	3	*Defined*
Seberapa efektif aktivitas tersebut dalam upaya melakukan perbaikan berkelanjutan?	Belum efektif	Aktivitas yang dilakukan oleh organisasi belum efektif dalam upaya melakukan perbaikan berkelanjutan karena. Tidak adanya audit internal secara berkala.	2	*Repeatable buat intuitive*
Apakah ada tim khusus yang menangani perbaikan dan peningkatan sistem?	Iya	Terdapat staf teknis dari diskominfotik yang menangani langsung masalah dan perubahan pada website.	3	*Defined*
Apakah setelah dilakukan perbaikan ada pelaporan kepada pihak terkait (misalnya Kabid atau pimpinan)?	Iya	Hasil perbaikan biasanya disampaikan secara langsung kepada atasan setelah selesai.	3	*Defined*
Apakah hasil perbaikan terhadap website e-wartawan terdokumentasikan secara resmi?	Tidak	Perbaikan langsung dilakukan tanpa pencatatan atau laporan formal.	0	*Non existent*
Apakah perbaikan terhadap celah keamanan dilakukan segera setelah ditemukan?	Iya	Jika ditemukan kerentanan atau error, langsung diperbaiki oleh tim teknis.	3	*Defined*
Apakah organisasi melakukan pelaporan hasil perbaikan kepada kepala bidang atau pimpinan?	Iya	Perbaikan yang dilakukan biasanya disampaikan langsung kepada atasan, meskipun tidak secara tertulis.	3	*Defined*
Score Maturity			**2,42**	

Sumber : Data Penelitian lapangan (2024)

Berdasarkan hasil pengumpulan data melalui kuesioner dan wawancara terhadap implementasi sub klausul perbaikan, pada sistem informasi dapat diketahui bahwa jumlah keseluruhan keamanan informasi memiliki maturity indeks sejumlah 2,42 berikut rumus bagi mencari score maturitasnya.

$$\text{Indeks Maturity} = \frac{17}{7} * 100\%$$

Hasil penjumlahan bagi score pertanyaan yang dijawab dengan 17 kemudian dibagi dengan 7 dengan banyaknya jumlah pertanyaan klausul maka dapatlah hasilnya 2,42 kemudian di kali 100% bagi mengalikan hasil pembagian dengan 100% cukup mengalikan hasil pembagian dengan 1 atau 100* dalam bentuk desimal yaitu 1. Langkah ini tidak akan mengubah nilai dari hasil pembagian sebelumnya, karena mengalikan dengan satu akan mendapatkan nilai yang sama.

4. METODE PENELITIAN

Berdasarkan hasil pengumpulan dan pengolahan data melalui metode wawancara, kuesioner, dan observasi langsung di Kantor Diskominfotik, dilakukan pengukuran terhadap tingkat keamanan informasi menggunakan standar ISO/IEC 27001. Penilaian dilakukan terhadap tujuh klausul utama, yaitu Klausul 4 sampai dengan klausul 10. Setiap klausul dianalisis dan diberikan skor maturity level berdasarkan jawaban dari responden serta dari bukti dokumentasi.

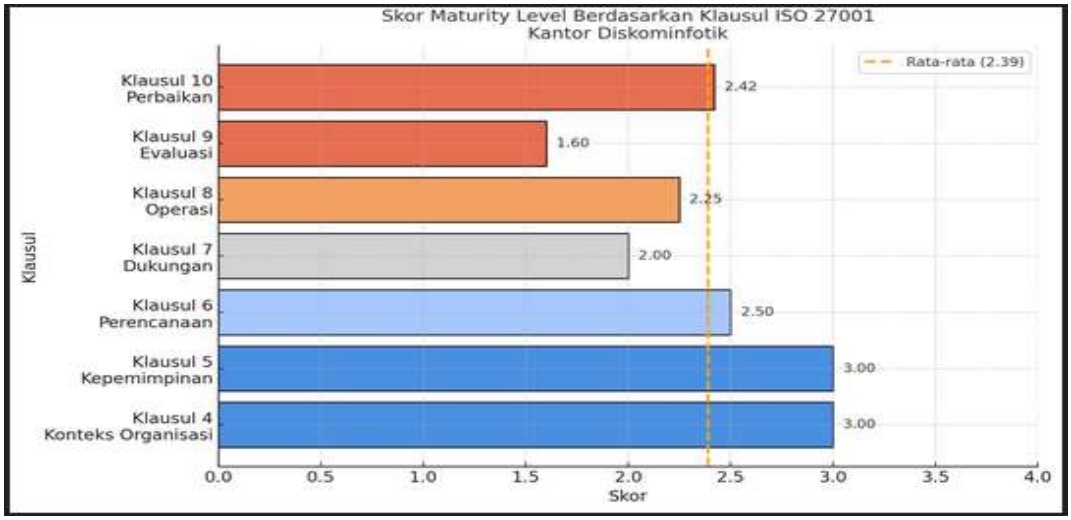
Berikut yakni rekapitulasi skor maturity level yang diperoleh:

Tabel 10. Rekapitulasi Skor Keamanan Informasi per Klausul ISO 27001

Klausul	Score
1. Klausul 4 : Konteks Organisasi	3
2. Klausul 5 : Kepemimpinan	3
3. Klausul 6 : Perencanaan	2.5
4. Klausul 7 : Dukungan	2
5. Klausul 8 : Operasi	2.25
6. Klausul 9 : Evaluasi	1.6
7. Klausul 10 : Perbaikan	2.42
Rata - rata	**2,39**

Sumber : Data Penelitian lapangan (2024)

Dari tabel diatas dapat dilihat klausul 4 (konteks organisasi) memperoleh skor tertinggi yaitu 3 diikuti oleh klausul 5 (kepemimpinan) dengan skor 3. Nilai tinggi klausul ini menunjukkan bahwa organisasi telah memiliki pemahaman yang baik terhadap lingkungan, serta menunjukkan peran yang aktif dan dukungan dari pimpinan dalam upaya penerapan keamanan informasi. Berdasarkan Tabel 4.2 di atas, maka diperoleh grafik yang menggambarkan skor keamanan informasi per klausul. Grafik ini menunjukkan adanya perbedaan antara klausul dengan tingkat kematangan tinggi dan rendah, yang kemudian menjadi dasar dalam penyusunan rekomendasi sistem.



Gambar 1. Grafik maturity level

Rekomendasi

Berdasarkan hasil evaluasi terhadap sistem e-wartawan menggunakan standar ISO/IEC 27001 dan pendekatan maturity level SSE-CMM, diperoleh skor rata-rata sebesar 2,39, yang menunjukkan bahwa sistem keamanan informasi pada website e-wartawan berada pada tingkat 2 – *Repeatable But Intuitive.* Artinya, proses keamanan telah dilakukan secara berulang, namun belum melibatkan dokumentasi secara formal. Maka, peneliti menyusun beberapa rekomendasi yaitu audit keamanan informasi secara berkala, menyusun dan mendokumentasikan SOP keamanan informasi, pelatihan keamanan informasi secara rutin, melakukan backup data secara rutin dan dokumen hasil perbaikan. Sebagai acuan bagi pihak diskominfotik dalam meningkatkan tingkat kematangan keamanan informasi dimasa mendatang.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil evaluasi terhadap sistem e-wartawan menggunakan standar ISO 27001, diperoleh rara-rata maturity level sebesar 2,39 yang menunjukkan bahwa sistem berada pada tingkat *repeatable* menuju *Defined.* Evaluasi dilakukan terhadap tujuh klausul ISO 27001, dengan hasil tertinggi pada klausul 4 dan 5. Selama penelitian diskominfotik telah melakukan perbaikan dengan menambahkan satu fitur pengajuan proposal sebagai upaya meningkatkan keamanan. Oleh karena itu, peneliti memberikan beberapa rekomendasi agar sistem e-wartawan dapat memenuhi prinsip keamanan informasi sesuai standar ISO 27001.

Saran Berdasarkan hasil dari penelitian tugas akhir ini, peneliti memberikan beberapa saran yang dapat dijadikan acuan bagi penelitian selanjutnya maupun pengembangan sistem di masa mendatang. Penelitian ini menggunakan framework ISO 27001 bagi mengevaluasi keamanan informasi, serta melakukan pengukuran tingkat kematangan menggunakan model

SSE-CMM (**Systems Security Engineering Capability Maturity Model)**. Oleh karena itu peneliti menyarankan khususnya diskominfotik melakukan audit secara berkala guna bagi mendeteksi celah atau kelemahan yang terjadi.

DAFTAR REFERENSI

Abdul, M., Ys, F., Zen, B. P., & Rini, D. E. W. (2023). Penerapan sistem manajemen keamanan informasi ISO 27001 pada Perpusnas RI dalam mendukung keamanan tata kelola teknologi informasi.

Alim, M., Munthe, I. R., Juledi, A. P., & Universitas Labuhan Batu. (2024). Evaluasi keamanan sistem informasi dalam lingkungan bisnis digital. Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI), 7(1), 328–332.

Analisis penerapan sistem manajemen keamanan informasi SIMHP BPKP menggunakan standar ISO 27001. (n.d.).

Daniswara, M. C., Putrawanto, D. I., Najib, M., Achmadha, Z., Chairul Adnani, M. S. I., & Mukaromah, S. (2023). Evaluasi keamanan informasi di lingkungan rumah sakit: Pendekatan audit ISO 27001 di RS Rahman Rahim Sidoarjo.

Evaluasi manajemen keamanan informasi. (n.d.). Dokumen internal.

Kornelia, A., & Irawan, D. (2021). Analisis keamanan informasi menggunakan tools Indeks KAMI ISO 4.1.

Manullang, A. F., & Harsono, L. D. (n.d.). Asesmen keamanan informasi menggunakan Indeks Keamanan Informasi (KAMI) pada institusi XYZ.

Musyarofah, S. R., & Bisma, R. (2021). Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001:2013 pada institusi pemerintah. Teknologi, 11(1), 1–5. https://doi.org/10.26594/teknologi.v11i1.2152

Program Studi Sistem Informasi & Sekolah Tinggi Manajemen Informatika Primakara. (n.d.). Pengukuran tingkat keamanan sistem informasi menggunakan Indeks KAMI versi 3.1, dan mengukur tingkat kerentanan server menggunakan Network Security Assessment (Studi kasus: Kominfo Kabupaten Gianyar).

Rahmah, Y., Hayuhardhika, W., Putra, N., & Herlambang, A. D. (2020). Evaluasi tingkat keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto dengan menggunakan Indeks KAMI. Retrieved from http://j-ptiik.ub.ac.id

Rahmi, M. N., Utamajaya, J. N., Hadisaputro, E. L., & Borneo Internasional, S. (2024). Evaluasi audit sistem informasi: Studi kasus pada perusahaan teknologi XYZ di Kota Balikpapan, 2(4). https://doi.org/10.61132/mars.v2i4.2560

Riana, E., Sulistyawati, M. E. S., & Putra, O. P. (2023). Analisis tingkat kematangan (maturity level) dan PDCA (Plan-Do-Check-Act) dalam penerapan audit sistem manajemen keamanan informasi pada PT Indonesia Game menggunakan metode ISO 27001:2013.

Journal of Information System Research (JOSH), 4(2), 632–640. https://doi.org/10.47065/josh.v4i2.2552

Riswaya, A. R., Sasongko, A., Maulana, A., Mardira Indonesia, S., & Universitas Langlangbuana Bandung. (2020). Evaluasi tata kelola keamanan teknologi informasi menggunakan Indeks KAMI bagi persiapan standar SNI ISO/IEC 27001 (Studi kasus: STMIK Mardira Indonesia). Jurnal Computech & Bisnis, 14(1), 10–18.

Sinaga, R. (n.d.). Penerapan ISO/IEC 27001:2022 dalam tata kelola keamanan sistem informasi: Evaluasi proses dan kendala. Retrieved from https://journal.fkom.uniku.ac.id/ilkom