# Pengembangan Dokumen Tata Kelola Keamanan Sistem Informasi dengan Standar ISO 27001: 2013 Pada Yayasan Dana Sosial Al-Falah Surabaya

1st Naufal Rakhmad Denisya Putra
*Sistem Informasi*
*Telkom University*
Surabaya, Indonesia
naufalrakhmad1408@gmail.com

2nd Muhammad Nasrullah
*Sistem Informasi*
*Telkom University*
Surabaya, Indonesia
emnasrul@telkomuniversity.ac.id

3rd Mustafa Kamal
*Teknologi Informasi*
*Telkom University*
Surabaya, Indonesia
Mustafakamal@telkomuniversity.ac.id

***Abstrak* — Yayasan Dana Sosial Al-Falah (YDSF) Surabaya merupakan Lembaga Amil Zakat Nasional yang telah memanfaatkan teknologi informasi dalam operasionalnya, namun masih menghadapi kendala serius terkait keamanan teknologi informasi dan pengelolaan aset digital. Berdasarkan hasil wawancara dan audit yang dilakukan oleh tim dari Telkom University Surabaya, ditemukan kelemahan serta kerentanan dalam tata kelola sistem informasi, terutama pada klausul Incident Management, Asset Management, dan Policy, yang memiliki skor di bawah rata-rata standar ISO 27001:2013. Penelitian ini bertujuan untuk mengembangkan dokumen tata kelola keamanan informasi sesuai standar tersebut guna meningkatkan keamanan dan efektivitas sistem informasi di YDSF. Metode penelitian yang digunakan adalah kualitatif deskriptif dengan teknik pengumpulan data berupa observasi lapangan, wawancara mendalam, serta telaah dokumen. Hasil penelitian menghasilkan 8 dokumen kebijakan, 9 dokumen SOP, dan 5 dokumen formulir terkait klausul tersebut. Selain itu, dilakukan analisis kesenjangan (gap analysis) antara kondisi aktual dengan standar ISO untuk menyesuaikan kebutuhan YDSF. Hasil ini diharapkan membantu menjaga integritas, kerahasiaan, ketersediaan informasi, dan meningkatkan kesiapan YDSF menghadapi ancaman keamanan informasi di masa mendatang.**

***Kata kunci*— Tata Kelola Kemanan Sistem Informasi, YDSF Surabaya, Keamanan Informasi Organisasi, Standar ISO 27001: 2013.**

## I. PENDAHULUAN

Kebutuhan dalam memanfaatkan teknologi informasi saat ini sudah menjadi kebutuhan bagi setiap individu, organisasi, dunia pendidikan, pemerintahan, dan dunia usaha. Pemanfaatan TI diperlukan untuk menunjang aktivitas proses bisnis dan menunjang kinerja organisasi [1]. Dengan semakin pesatnya perkembangan teknologi, saat ini informasi semakin banyak diproses dan disimpan. Oleh karena itu, organisasi harus mengembangkan kebijakan atau aturan yang dapat mengatur penggunaan teknologi informasi oleh organisasi untuk memastikan bahwa informasi organisasi terlindungi dari ancaman keamanan informasi [2].

Yayasan Dana Sosial Al-Falah (YDSF) Surabaya merupakan Lembaga Amil Zakat Nasional yang memanfaatkan teknologi informasi untuk mengelola data sensitif seperti informasi keuangan donatur dan data penerima manfaat [2]. Namun, hasil wawancara dan audit oleh Telkom University Surabaya menunjukkan adanya kekurangan dalam tata kelola keamanan sistem informasi, termasuk sistem yang belum terintegrasi, kebijakan dan SOP yang belum optimal, serta lemahnya pengamanan data. Beberapa insiden seperti kebocoran data dan hilangnya aset terjadi akibat kurangnya regulasi [3].

Dari tujuh klausul yang diaudit, tiga klausul yaitu Incident Management, Asset Management, dan Policy menunjukkan kekurangan dan kerentanan dalam tata kelola keamanan informasi yang digunakan.

Berdasarkan dari klausul Incident Management dapat diartikan bahwa dalam klausul ini terdapat atribut IM1 (Prepare) dengan nilai 2,4, IM2 (Identify) dengan nilai 2,4, IM6 (Learn) dengan nilai 2,2. Nilai tersebut termasuk dibawah nilai rata-rata klausul Incident Management yakni 2,53. Sedangkan pada atribut IM3 (React) dengan nilai 2,636, IM4 (Manage and Contain) dengan nilai 2,636, IM5 (Resolve) dengan nilai 2,8 sudah mendapat nilai baik, namun masih perlu ditingkatkan kembali.

Berdasarkan dari klausul Asset Management dapat diartikan bahwa dalam klausul ini terdapat atribut AM1 (Inventory) dengan nilai 2,8, nilai tersebut sudah dikatakan baik karena memenuhi nilai rata-rata dari klausul Asset Management dengan nilai 2,69, tetapi klausul tersebut masih dapat ditingkatkan kembali. Sedangkan pada atribut AM2 (Classification) dengan nilai 2,654, dan AM3 (Ownership) dengan nilai 2,618 masih belum memenuhi rata-rata dari klausul Asset Management, sehingga masih diperlukan perbaikan.

Berdasarkan dari klausul Policy dapat diartikan bahwa pada atribut P1 (Policies) dengan nilai 2,545, P3 (Guidelines & Procedure) dengan nilai 2,6, P4 (Principles & Axiom) dengan nilai 2,527 sudah baik karena sudah memenuhi standar nilai yakni 2,536, tetapi masih perlu ditingkatkan

lebih baik lagi. Sedangkan pada atribut P2 (Standard) dengan nilai 2,472 belum memenuhi kriteria nilai dari klausul Policy.

Dengan hasil keseluruhan, bahwa klausul nilai pada klausul *Compliance, Risk Management, Physical & Environmental, dan Access Control* sudah menunjukkan memenuhi standar nilai rata-rata. Sedangkan pada klausul *Incident Management, Asset Management, dan Policy* masih perlu perbaikan dan peningkatan. Maka dari itu, dalam penelitian ini melanjutkan dari hasil audit sebelumnya yang dimana perlu pengembangan dokumen tata kelola keamanan sistem informasi dengan melakukan analisis kesenjangan antara kondisi keadaan aktual dengan kondisi yang diharapkan berdasarkan ISO 27001: 2013 yang memuat persyaratan yang dibutuhkan organisasi untuk membantu pengelolaan kebijakan, standar, dan sasaran keamanan sistem informasi yang bertujuan dapat melindungi dari terjadinya insiden atau permasalahan pada keamanan sistem informasi YDSF Surabaya. Selain itu, dapat digunakan di berbagai jenis organisasi, berfokus melindungi aset informasi, dan membantu organisasi untuk mengetahui tingkat keamanan teknologi informasi yang dimiliki dan tahapan peningkatan yang perlu dilakukan pada keamanan informasi. Kami harap pengembangan dokumen ini dapat menjadi panduan penting dalam suatu aktivitas yang berhubungan dengan keamanan sistem informasi, sehingga pelayanan yang diberikan YDSF Surabaya dapat berjalan maksimal.

## II. KAJIAN TEORI

Pada tahap ini akan membahas mengenai teori yang berhubungan dengan topik penelitian tugas akhir ini.

### A. Yayasan Dana Sosial Al-Falah Surabaya

Yayasan Dana Sosial Al-Falah atau bisa disebut dengan YDSF adalah Lembaga Amil Zakat Nasional (LAZNAS) mengelola dana zakat dan infak/sedekah untuk didistribusikan kepada pihak yang sangat membutuhkan sehingga lembaga ini diharapkan mampu membantu negara dalam mengatasi masalah kemanusiaan yang universal [4]. YDSF berkantor pusat di Jl. Kertajaya 9-C/17, Kertajaya, Gubeng, Surabaya, Jawa Timur. Dalam pelaksanaannya, YDSF memiliki berbagai program yaitu pada bidang pendidikan, dakwah, pemberdayaan yatim dan dhuafa, sosial kemanusiaan, dan pemakmuran masjid [5]. Pada penitian ini, akan bekerjasama dengan divisi Markom & IT YDSF Surabaya untuk melakukan pengembangan dokumen tata kelola keamanan informasi. Tujuannya adalah untuk membantu pengelolaan kebijakan, standar, dan sasaran keamanan sistem informasi untuk melindungi dari terjadinya permasalahan pada keamanan sistem informasi YDSF Surabaya.

### B. Sistem Informasi

Sistem Inforamsi menjelaskan mengenai pengertian, komponen, dan fungsi dari sistem informasi. Sistem Informasi diambil dari 2 pengertian, yakni sistem sekaligus data dan informasi [6]. Sistem secara umum adalah kesatuan dari komponen atau elemen yang saling berinteraksi dan bekerja sama untuk mencapai tujuan tertentu. Sistem ditemukan dalam berbagai konteks, yaitu sistem biologis, sistem sosial, sistem mekanik, dan sistem informasi [7]. Sedangkan data dan informasi adalah dua konsep yang saling berkaitan, akan tetapi memiliki perbedaan mendasar dalam konteks sistem informasi [8]. Data adalah kondisi saat ini yang dapat dideskripsikan dengan benda, kejadian, aktivitas, dan transaksi. Informasi adalah data yang sudah diolah dan dapat digunakan sebagai dasar pengambilan keputusan. Sehingga pengertian sistem informasi adalah kesatuaan yang terdiri dari perangkat keras, perangkat lunak, manusia, data, dan prosedur yang bekerja terintegrasi untuk mengumpulkan, mengolah, menyimpan, dan mendistribusikan untuk mendukung pengambilan keputusan [9].

### C. Sistem Manajemen Keamanan Informasi

Teori ini menjelaskan mengenai kerangka kerja yang digunakan untuk keamanan informasi organisasi. Dimana membahas mengenai dasar pengertian terkait sistem manajemen keamanan informasi. Keamanan sistem informasi sendiri adalah disiplin ilmu praktik yang berfokus pada perlindungan integritas, kerahasiaan, dan ketersediaan informasi dalam suatu sistem [10]. Triad keamanan sistem informasi terdiri dari integritas, kerahasiaan, dan ketersediaan yang membentuk fondasi dasar untuk pemahaman konsep keamanan. Sedangkan sistem manajemen keamanan informasi (SMKI) memiliki arti suatu kerangka kerja yang dirancang untuk menentukan bagian penting yang berpengaruh terhadap organisasi dan pembagian kontrol keamanan yang dapat digunakan untuk melindungi informasi sebagai aset dan menjamin kerahasiaan pihak lain [11].

### D. Tata Kelola Keamanan Sistem Informasi

Berdasarkan definisi Tata Kelola Keamanan Sistem Informasi menurut beberapa sumber menjelaskan, yaitu suatu bagian turunan dari tata kelola perusahaan yang terdiri atas kepemimpinan, struktur, proses, organisasional yang memastikan bahwa organisasi berlanjut serta meningkatkan tujuan dan strategi [12]. Sedangkan menurut [13], yaitu suatu cabang dari tata kelola perusahaan yang tefokus pada sistem teknologi informasi (IT) serta manajemen kinerja dan risikonya. Ada 11 kontrol penting dalam tata kelola keamanan sistem informasi pada sebuah organisasi untuk melakukan pengukuran atau evaluasi. Berikut penjelasan dari 11 kontrol tersebut:

1.) *Information Security Policy,* memberikan arahan mengenai pentingnya sebuah keamanan sistem informasi dalam organisasi.
2.) *Communication & Operations Management,* menentukan suatu kebijakan keamanan sistem informasi dan memvalidasi dalam prosedur operasional, kontrol, dan tanggung jawab yang telah ditetapkan.
3.) *Acces Control,* sebagai sistem yang mendapatkan otoritas dalam organisasi untuk mengontrol akses ke area dan sumber daya tertentu atau sistem informasi berbasis komputer.
4.) *Information System Acquisition, Development an Maintenance,* sebuah proses mengembangkan dan memelihara sistem informasi.
5.) *Organization of Information Security,* sebagai struktur dalam organisasi yang menerapkan komitmen manajemen terhadap keamanan sistem informasi.
6.) *Asset Management,* melakukan pengamanan, pengidentifikasian, melacak, mengelompokkan, dan

menetapkan kepemilikan aset yang penting dalam organisasi.

7.) *Information Security Incident Management,* untuk melakukan antisipasi terhadap insiden yang terjadi dalam organisasi.
8.) *Business Continuity Incident Management,* memastikan keberlangsungan operasional dalam situasi abnormal yang tidak semestinya terjadi.
9.) *Human Resources Security,* memastikan bahwa seluruh karyawan telah memenuhi syarat dan paham atas peran dan tanggung jawab dalam organisasi.
10.) *Physical and Environment Security,* melindungi sistem, bangunan dan infrastuktur pendukung terkait ancaman yang terjadi dengan lingkungan fisik maupun sistem informasi dan teknologi informasi.
11.) *Compliance,* melibatkan terhadap peraturan, undang-undang, dan kepatuhan terhadap kebijakan, standar, dan proses keamanan.

Sehingga dapat disimpulkan, tata kelola keamanan sistem informasi adalah kerangka kerja yang mendefinisikan aturan, kebijakan, dan prosedur yang diperlukan untuk memastikan bahwa keamanan sistem informasi dalam suatu organisasi dikelola dengan baik.

## E. Dokumen Standar Keamanan Sistem Informasi

Dokumen standar keamanan sistem informasi adalah instrumen tertulis yang menyediakan panduan, aturan, dan prosedur untuk memastikan bahwa keamanan sistem informasi pada suatu organisasi diatur dan dikelola dengan efektif [14]. Teori ini melibatkan konsep dan prinsip yang bertujuan untuk menciptakan lingkungan yang aman bagi pengelolaan informasi [15].


**Gambar 1 Struktur Dokumen SMKI** [15]

Pada gambar diatas, SMKI memiliki struktur dokumen berupa hirarki yang terdiri dari tiga tingkatan [16]. Dokumen tingkat I (bersifat strategis), yang memuat dokumen kebijakan, standar, sasaran, dan rencana terkait peningkatan SMKI. Dokumen tingkat II (bersifat opsional), memuat prosedur dan panduan yang telah dikembangkan organisasi secara internal dan penerapan kebijakan yang telah ditetapkan. Dokumen tingkat III (bersifat opsional), memuat instruksi kerja, petunjuk teknis, dan formulir pendukung dalam pelaksanaan prosedur sampai ketingkat teknis.

## F. ISO 27001: 2013

Standar ISO 27001: 2013 memberikan kerangka khusus untuk menyediakan persyaratan untuk penetapan, penerapan, pemeliharaan, dan perbaikan berkelanjutan terhadap sistem manajemen keamanan informasi (SMKI) [10]. Dimana memiliki 14 Aspek (Klausul), 35 kontrol Objektif, dan 114 kontrol keamanan [17]. Jika SMKI baik, maka akan membantu pengamanan dan perlindungan terhadap ancaman yang dapat mengganggu aktifitas bisnis, dan mengamankan proses bisnis agar terlindungi dari risiko kerugian atau kegagalan pada keamanan sistem informasi [18].

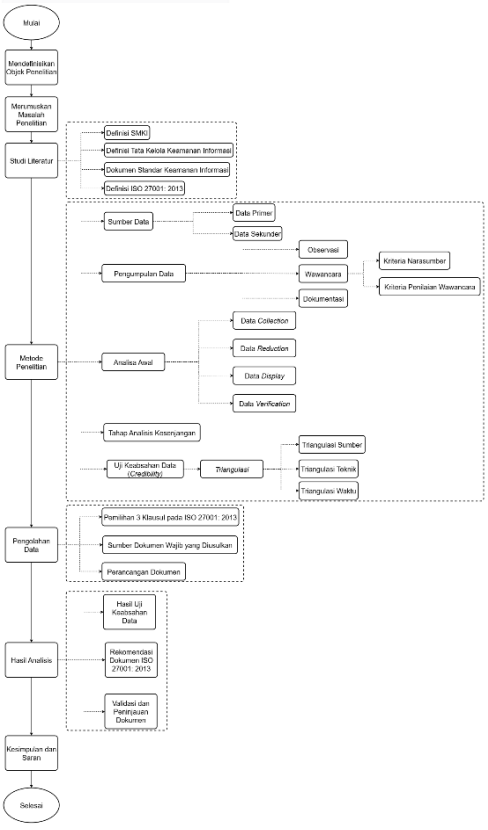
Sehingga dapat diartikan bahwa, ISO 27001: 2013 adalah standar keamanan yang digunakan organisasi dalam membuat kebijakan organisasi, dengan melakukan pengidentifikasian risiko dan pemeriksaan terhadap pelaksanaan yang telah diterapkan. Penelitian ini menggunakan standar ISO 27001: 2013 karena digunakan di berbagai jenis organisasi, berfokus melindungi aset informasi, dan membantu organisasi untuk mengetahui tingkat keamanan informasi yang dimiliki serta tahapan peningkatan yang perlu dilakukan.

## G. Analisis Kesenjangan

Analisis Kesenjangan atau *gap analysis* adalah untuk mengetahui seberapa besar kesenjangan antara kondisi aktual dengan kondisi yang diharapkan, serta mengetahui peningkatan kinerja yang diperlukan untuk menutupi kesenjangan yang terjadi [16]. Tujuan dari analisis kesenjangan berguna agar pihak manajemen bisa mengidentifikasi kondisi organisasi saat ini dengan kondisi yang diharapkan organisasi serta pertumbuhan yang diinginkan antara as-is dan to-be.

# III. METODE

Pada tahap ini membahas mengenai gambaran rancangan penelitian yang meliputi prosedur atau langkah-langkah penelitian, waktu penelitian, sumber data, cara perolehan data dan menjelaskan metode yang akan digunakan dalam penelitian. Gambar dibawah ini merupakan alur penilitian yang digunakan untuk menyelesaikan permasalahan yang diangkat.




**Gambar 2 Alur Penelitian**

A. Metode Kualitatif Deskriptif

Penelitian ini menggunakan metode deskriptif kualitatif. Dimana memberikan gambaran dan penjelasan yang tepat mengenai keadaan dan permasalahan yang dihadapi. Metode penelitian deskriptif kualitatif digunakan untuk meneliti pada kondisi objek yang alamiah. Digunakannya metode deskriptif kualitatif ini bermaksud untuk memahami lebih mendalam dan mendeskripsikan terkait pengembangan dokumen tata kelola keamanan informasi yang penting dilakukan pada YDSF Surabaya. Data yang dikumpulkan pada penelitian ini adalah mengenai kondisi tata kelola keamanan informasi saat ini pada YDSF Surabaya dan kondisi yang diharapkan berdasarkan standar ISO 27001: 2013. Hasilnya kemudian dianalisis dan dilakukan perbandingan dengan kondisi yang diharapkan berdasarkan standar ISO 27001: 2013 sehingga menghasilkan rekomendasi dokumen yang valid.

B. Sumber Data

Sumber data dalam penelitian ini ada dua macam bentuk, yaitu sumber data primer dan sumber data sekunder. Data primer yaitu data yang diambil secara langsung. Data primer dalam penelitian ini didapat melalui jawaban dari wawancara dengan narasumber yang bertujuan untuk mengumpulkan informasi mengenai kondisi tata kelola keamanan informasi yang akan dilakukan penyesuaian dengan standar ISO 27001: 2013 pada YDSF Surabaya. Sedangkan data sekunder adalah data yang sudah tersedia dan dikumpulkan oleh orang diluar peneliti dan data yang asli. Data sekunder dalam penelitian ini yaitu diambil dari hasil audit tata kelola keamanan informasi yang dilakukan oleh *Telkom University,* karya ilmiah, buku standar ISO 27001: 2013, dan jurnal-jurnal lain pendukung penelitian ini. Dengan tujuan mendapat pemahaman yang mendalam mengenai permasalahan yang terjadi terkait tata kelola keamanan informasi pada YDSF Surabaya.

C. Teknik Pengumpulan Data

Dalam menentukan data yang diperlukan, perlu dilakukan teknik pengumpulan data agar bukti dan fakta yang diperoleh menjadi obyektif dan valid serta tidak terjadi penyimpangan dari keadaan yang sebenarnya [19]. Dalam mengumpulkan data pada penelitian ini, dilakukan dengan 3 tahap, yaitu observasi, wawancara, dan dokumentasi.

Pada tahap observasi adalah cara untuk mengamati, mengumpukan data terhadap objek secara langsung maupun tidak langsung. Proses observasi dalam penelitian ini yaitu kendala terkait bidang IT yang terjadi pada YDSF Surabaya dan bagaimana pihak tim IT YDSF dalam menghadapi kendala tersebut yang berkaitan dengan IT.

Pada tahap wawancara dilakukan untuk mengumpulkan data yang beragam dari responden dalam berbagai situasi dan konteks serta agar mampu mengajukan pertanyaan dengan bertatap muka langsung dengan narasumber sekaligus mendapatkan jawaban secara rinci dari pertanyaan yang diajukan [20]. Pada penelitian ini, kriteria narasumber yang diambil adalah yang profesional dalam bidang IT. Narasumber dari penelitian ini yaitu bapak Sachroni Gumilar selaku senior manajer IT YDSF Surabaya dan bapak Khairul Anam selaku staf IT YDSF Surabaya.

Wawancara yang dilakukan dalam penelitian ini adalah wawancara semi terstruktur yang dimana mempersiapkan pertanyaan terlebih dahulu yang kemudian diajukan ke narasumber, agar tidak menimbulkan pertanyaan bebas yang tidak baik [21].

Pada tahap dokumentasi yaitu pelengkap dari observasi dan wawancara mengenai catatan peristiwa yang sudah berlalu [22]. Hal yang berkaitan adalah data tentang gambaran umum YDSF Surabaya yang digunakan untuk melengkapi data. Sedangkan dokumentasi lainnya seperti data-data tertulis dan template dokumen yang dimiliki oleh YDSF Surabaya.

D. Analisis Data

Analisis data yaitu proses mencari dan menyusun data yang diperoleh melalui teknik pengumpulan data dengan cara mengorganisasikan data ke kategori, menjabarkan, dan membuat kesimpulan agar data mudah dipahami oleh diri sendiri maupun orang lain [23]. Adapun langkah-langkah yang diambil dalam analisis data, yaitu data *collection,* data *reduction,* data *display,* dan *conclusing drawing / verification.* Data *collection* membahas mengenai permasalahan terkait tata kelola keamanan informasi yang terjadi pada YDSF Surabaya. Data *reduction* yaitu merangkum data dengan menentukan kebutuhan dalam pengembangan tata kelola keamanan informasi pada YDSF Surabaya. Data *display* membahas penyajian data mengenai kebutuhan dokumen yang diperlukan terkait tata kelola keamanan inforamsi pada YDSF Surabaya. Dan yang terkahir yaitu *conclusing drawing / verification,* yang menghasilkan temuan-temuan baru terkait pengembangan dokumen yang sebelumnya belum ada atau belum terstruktur yang dimana setelah dilakukan pengembangan dokumen dalam penelitian diharapkan ada peningkatan terkait tata kelola keamanan informasi pada YDSF Surabaya.

E. Uji Keabsahan Data

Uji keabsahan data dilakukan untuk memastikan data dalam penilitian ini valid, kredibel, dan dapat dipertanggung jawabkan. Keabsahan data dalam penelitian ini menggunakan uji kredibilitas yang bertujuan untuk uji kepercayaan data hasil penelitian yang sudah dilakukan. Dalam menguji kredibilitas, penelitian ini menggunakan teknik triangulasi yang dimana ada 3 teknik didalamnya, diantaranya triangulasi sumber, yaitu membandingkan data dari berbagai narasumber. Triangulasi teknik, yaitu memeriksa data yang sama dengan teknik yang berbeda. Dan terakhir triangulasi waktu, yaitu pemeriksaan ulang informasi pada waktu dan situasi yang berbeda untuk melihat konsistensi data.

## IV. HASIL DAN PEMBAHASAN

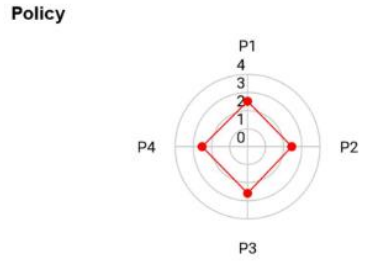
Pada tahap ini membahas mengenai hasil dari pembahasan metode penelitian. Hasil dan pembahasan mengenai penelitian ini yaitu pengembangan dokumen terkait tata kelola keamanan informasi dari usulan dokumen wajib yang diusulkan berdasarkan standar ISO 27001: 2013 dan beberapa referensi jurnal.

A. Pemilihan 3 Klausul Pada ISO 27001: 2013

Penelitian ini mengambil tiga klausul yakni *Information Security Policy, Asset Management,* dan *Information Security Incident Management* pada standar ISO 27001: 2013 dari hasil audit yang dilakukan oleh *Telkom University* yang dimana nilai audit keamanan informasi dari tiga klausul tersebut masih belum memenuhi standar nilai yang

ditetapkan, sehingga menunjukkan kekurangan dan kerentanan dalam tata kelola keamanan informasi yang digunakan oleh YDSF Surabaya [3]. Adapun hasil dari audit yang dilakukan sebagai berikut:

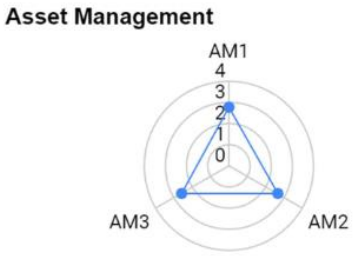
1.) Klausul A.5 *Information Security Policy* (Kebijakan Keamanan Informasi)




**Gambar 3 Radar Chart Klausul A.5** [3]

Pada gambar *radat chart* klausul A.5 menjelaskan bahwa atribut (P1) *Policies* dengan nilai 2,545, atribut (P3) *Guidelines & Procedure* dengan nilai 2,6, dan atribut (P4) *Principles & Axiom* dengan nilai 2,527 sudah baik karena sudah memenuhi nilai standar yaitu 2,5. Tetapi masih perlu ditingkatkan lebih baik lagi. Sedangkan pada atribut (P2) *Standar* dengan nilai 2,472 belum memenuhi kriteria nilai dari klausul *Policy* dengan nilai 2,5. Sehingga masih perlu perbaikan.

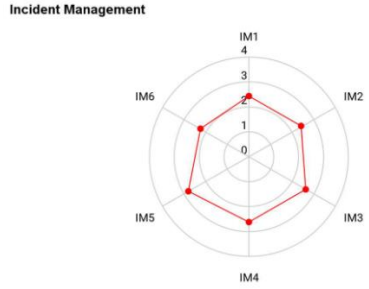
2.) Klausul A.8 *Asset Management* (Manajemen Aset)




**Gambar 4 Radar Chart Klausul A.8** [3]

Pada gambar *radar chart* klausul A.8 menjelaskan bahwa atribut (AM1) *Inventory* dengan nilai 2,8. Nilai tersebut sudah dikatakan baik, karena memenuhi nilai standar dari klausul *Asset Management* yakni 2,7. Tetapi klausul tersebut masih dapat ditingkatkan kembali. Sedangkan pada atribut (AM2) *Classification* dengan nilai 2,654 dan atribut (AM3) *Ownership* dengan nilai 2,618 masih belum memenuhi rata-rata nilai standar dari klausul *Asset Management* dengan nilai 2,7, sehingga masih diperlukan perbaikan.

3.) Klausul A.16 *Information Security Incident Management* (Manajemen Insiden Keamanan Informasi)




**Gambar 5 Radar Chart Klausul A.16** [3]

Pada gambar *radar chart* klausul A.16 menjelaskan bahwa atribut (IM3) *React* dengan nilai 2,6 sudah mendapat nilai baik. Sedangkan pada atribut (IM1) *Prepare* dengan nilai 2,4, (IM2) *Identify* dengan nilai 2,4, dan (IM6) *Learn* dengan nillai 2,2, dimana nilai tersebut termasuk dibawah nilai standar klausul *Incident Management* yakni 2,5, sehingga masih perlu perbaikan. Pada atribut IM4 (*Manage and Contain*) dengan nilai 2,636, IM5 (*Resolve*) dengan nilai 2,8 sudah mendapat nilai baik, namun masih perlu ditingkatkan kembali.

B. Perancangan Dokumen Kebijakan

Pembuatan dokumen kebijakan ini mengacu pada standar ISO 27001: 2013, referensi jurnal, dan beberapa sumber lainnya, serta dasar hukum yang dijadikan pedoman penyusunan dokumen kebijakan di organisasi. Dalam perancangan struktur dokumen tidak keseluruhan mengacu pada standar tersebut, akan tetapi menyesuaikan dengan kebutuhan yang ada pada YDSF Surabaya. Struktur dokumen yang disusun, selanjutnya diberikan kepada pihak YDSF Surabaya sebagai rekomendasi dokumen keamanan informasi Pada tabel dibawah ini merupakan rancangan pengembangan dokumen setelah dilakukan analisis awal.

**Tabel 1 Hasil Perancangan Dokumen**

| Klausul | Dokumen Kebijakan |
|---|---|
| Information Security Policy (Kebijakan Keamanan Informasi) | Dokumen Kebijakan Kemanan Informasi Utama |
| | Dokumen Monitoring Penggunaan Teknologi Informasi |
| | Dokumen Kebijakan Penyimpanan dan Penghancuran Informasi |
| Asset Management | Dokumen Kebijakan Manajemen Aset Informasi |
| | Dokumen Prosedur Penilaian Risiko Aset Informasi |
| Information Security Incident Management | Dokumen Kebijakan Penanganan Insiden Keamanan Informasi |
| | Dokumen Prosedur Penanganan Insiden Keamanan Informasi |
| | Dokumen Daftar Insiden Keamanan Informasi |

C. Hasil Uji Keabsahan Data

Berdasarkan hasil dari wawancara diperoleh informasi bahwa divisi Teknologi Informasi (IT) pada Yayasan Dana Sosial Al-Falah (YDSF) Surabaya memegang peranan penting dalam mendukung operasional dan pengembangan layanan digital lembaga. YDSF aktif dalam memanfaatkan platform digital untuk memudahkan donatur dalam menyalurkan zakat, infak, dan sedekah. YDSF aktif dalam memanfaatkan platform digital untuk memudahkan donatur dalam menyalurkan zakat, infak, dan sedekah melalui situs resmi mereka, ydsf.org. Salah satu contoh nyata adalah kolaborasi antara YDSF dan Institut Teknologi Telkom Surabaya pada September 2023. Kerja sama ini bertujuan

untuk meningkatkan kualitas konten video tausyiah pendek yang disajikan secara online, menunjukkan upaya YDSF dalam memanfaatkan teknologi digital untuk memperluas jangkauan dakwah dan edukasi Islam kepada masyarakat luas.

Akan tetapi, pengelolaan Teknologi Informasi di YDSF masih menghadapi kendala, ada dari sistem yang belum terintegrasi, kebijakan dan SOP yang belum berjalan optimal, hingga lemahnya pengamanan penyimpanan data. Beberapa insiden seperti kebocoran data dan hilangnya aset terjadi akibat kurangnya regulasi dan penerapan prosedur. Meski demikian, YDSF telah memanfaatkan media digital untuk publikasi, dan memiliki sistem penyimpanan data otomatis. Namun, pelaksanaan proses bisnis dan pengelolaan aset masih perlu ditingkatkan agar sejalan dengan standar yang diharapkan.

D. Pengembangan Dokumen ISO 27001: 2013

Berdasarkan hasil identifikasi kebutuhan dokumen yang telah dilakukan menghasilkan Standard Operasional Prosedur beserta Formulirnya. Identifikasi tidak menghasilkan dokumen Instruksi Kerja, karena pada Standar Operasional Prosedur sudah menguraikan langkah aktivitas yang jelas dan mudah dipahami penanggung jawab kegiatan yang sudah disesuaikan dengan template Standar Operasional Prosedur yang sudah ada pada YDSF Surabaya. Beberapa dokumen yang dihasilkan terdapat pada tabel dibawah ini.

**Tabel 2 Hasil Identifikasi Kebutuhan Dokumen**

| Aspek | Kebutuhan Dokumen | Standar Operasional Prosedur | Formulir |
|---|---|---|---|
| *Information Security Policy* (Kebijakan Keamanan Informasi) | 1. Dokumen Kebijakan Keamanan Sistem Informasi<br>2. Dokumen Kebijakan Penyimpanan dan Penghancuran Informasi<br>3. Dokumen Monitoring Penggunaan Teknologi Informasi | 1. SOP Penetapan dan Peninjauan Kebijakan Keamanan Informasi<br>2. SOP Pelaksanaan Monitoring Penggunaan Teknologi Informasi<br>3. SOP Kebijakan Penyimpanan dan Penghancuran Informasi<br>4. SOP Evaluasi dan Audit Internal | 1. Formulir Pelaksanaan Monitoring Penggunaan Teknologi Informasi<br>2. Formulir Evaluasi dan Audit Internal |
| *Asset Management* (Manajemen Aset) | 1. Dokumen Kebijakan Manajemen Aset Informasi<br>2. Dokumen Prosedur Penilaian Risiko Aset Informasi | 1. SOP Penetapan dan Peninjauan Kebijakan Manajemen Aset Inforamsi<br>2. SOP Penilaian Risiko Aset Informasi | 1. Formulir Penilaian Risiko Aset Informasi |
| *Information Security Incident Management* (Manajemen Insiden Keamanan Informasi) | 1. Dokumen Kebijakan Penanganan Insiden Keamanan Informasi<br>2. Dokumen Prosedur Penanganan Insiden Keamanan Informasi<br>3. Dokumen Daftar Insiden Keamanan Informasi | 1. SOP Penetapan dan Peninjauan Kebijakan Penanganan Insiden Keamanan Informasi<br>2. SOP Prosedur Penanganan Insiden Keamanan Informasi<br>3. SOP Dokumentasi dan Pelaporan Insiden Keamanan Informasi | 1. Formulir Penanganan Insiden Keamanan Informasi<br>2. Formulir Dokumentasi Insiden Keamanan Informasi |

E. Hasil Pengembangan Dokumen, SOP, dan Formulir Monitoring Penggunaan IT

Pada tahap pengembangan dokumen, SOP, dan formulir monitoring penggunaan IT mengacu pada standar ISO 27001: 2013 dan referensi jurnal. Format penulisan serta konten isi dokumen, SOP, dan formulir mengikuti ketentuan yang dimiliki oleh YDSF Surabaya. Salah satu contoh dari hasil pengembangan dokumen yang telah dibuat akan dibahas pada bab ini.

Langkah awal saat dilakukan membuat dokumen, SOP, dan formulir adalah dengan diskusi terkait format dan poin yang perlu diisi dalam dokumen, SOP, dan formulir. Bertujuan untuk mengetahui informasi yang perlu ditulis pada penulisan dokumen kebijakan, SOP, dan formulir. Setelah itu, melakukan analisis terkait atribut dan kontrol pada standa ISO 27001: 2013 untuk memperoleh panduan yang dibutuhkan dalam pengembangan dokumen, SOP, dan formulir.

Hasil melakukan analisis ditulis dalam bentuk dokumen kebijakan monitoring penggunaan IT. Hasil dari dokumen kebijakan monitoring penggunaan IT, dibentuk dalam Standar Operasional Prosedur serta formulir yang dibutuhkan menyesuaikan format dari YDSF Surabaya. Dokumen, SOP, dan formulir yang telah dilakukan pengembangan, selanjutnya dilakukan peninjauan dan persetujuan oleh tim IT YDSF Surabaya.

## V. KESIMPULAN

Berdasarkan dari hasil pengembangan dokumen yang mengacu pada klausul *Information Security Policy, Asset Management,* dan *Information Security Incident Management* standar ISO 27001: 2013 pada Yayasan Dana Sosial Al-Falah Surabaya dapat disimpulkan bahwa proses pada klausul A.5 kebijakan keamanan informasi menghasilkan 3 dokumen, yaitu dokumen kebijakan keamanan sistem informasi, dokumen kebijakan penyimpanan dan penghancuran informasi, dan dokumen monitoring peggunaan teknologi informasi.Untuk SOP menghasilkan 4, yaitu SOP penetapan dan kebijakan keamanan informasi, SOP pelaksanaan monitoring

penggunaan teknologi informasi, SOP kebijakan penyimpanan dan penghancuran informasi, dan SOP evaluasi dan audit internal. Untuk formulir menghasilkan 2, yaitu formulir pelaksanaan monitoring penggunaan IT dan formulir evaluasi dan audit internal. Proses pada klausul A.8 Manajemen Aset menghasilkan 2 dokumen, yaitu dokumen kebijakan manajemen aset informasi dan dokumen prosedur penilaian risiko aset informasi. Untuk SOP menghasilkan 2 SOP, yaitu SOP penetapan dan peninjauan kebijakan manajemen aset informasi, dan SOP penilaian risiko aset informasi. Untuk formulir menghasilkan 1, yaitu formulir penilaian risiko aset informasi. Proses pada klausul A.16 manajemen insiden keamanan informasi menghasilkan 3 dokumen, yaitu dokumen kebijakan penanganan insiden keamanan informasi, dokumen prosedur penanganan insiden keamanan informasi, dan dokumen daftar insiden keamanan informasi.Untuk SOP menghasilkan 3, yaitu SOP penetapan dan peninjauan kebijakan penanganan insiden keamanan informasi, SOP prosedur penanganan insiden keamanan informasi, dan SOP dokumetasi dan pelaporan insiden keamanan informasi. Untuk formulir menghasilkan 2, yaitu formulir penanganan insiden keamanan informasi dan formulir dokumentasi insiden keamanan informasi. Sehingga dari pengembangan dokumen yang dihasilkan dapat digunakan untuk memberikan acuan langkah dalam melakukan tindakan selanjutnya serta bisa menjadi dasar untuk meningkatkan keamanan sistem informasi yang terdiri dari integritas, kerahasiaan, dan ketersediaan informasi pada lingkungan Yayasan Dana Sosial Al-Falah Surabaya dalam kesiapan menghadapi risiko keamanan informasi di masa depan.

## REFERENSI


[1] W. C. Pamungkas and F. T. Saputra, “Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013,” *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 101, 2020, doi: 10.30865/json.v1i2.1924.

[2] E. A. Putri, “Implementasi good corporate governance di Lembaga Amil Zakat Yayasan Dana Sosial Al-Falah (YDSF) Kota Malang,” 2018.

[3] M. F. Iso, M. Nasrulllah, S. Kom, M. Kom, Y. Sudianto, and S. K. M. Kom, “Laporan Hasil Audit Sistem Informasi Yayasan Dana Sosial Al-Falah IT Telkom Surabaya Surabaya,” 2023.

[4] Jauharatun Nisail Hikmah, “Manajemen Risiko Pada Pengelolaan Dana Zakat Di Lembaga Amil Zakat YDSF (Yayasan Dana Sosial Al-Falah) Jember,” *Islam. Econ. Financ. Focus*, vol. 2, no. 3, pp. 455–464, 2020.

[5] R. A. Fadilla, “Analisis Akuntabilitas Pengelolaan Dana Zakat Pada Yayasan Dana Sosial Al-Falah (Ydsf) Kota Malang,” pp. 1–127, 2018.

[6] D. P. Haqqi, K. Ghozali, and R. V. H. Ginardi, “Evaluasi Tata Kelola Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2013 dengan Menggunakan Model SSE-CMM (System Security Engineering Capability Maturity Model) pada Perusahaan Daerah Air Minum Surya Sembada Kota Surabaya,” *J. Tek. ITS*, vol. 11, no. 2, 2022, doi: 10.12962/j23373539.v11i2.91532.

[7] B. Panjaitan, L. Abdurrahman, and R. Mulyana, “Pengembangan Implementasi Sistem Manajemen Keamanan Informasi Berbasis Iso 27001 : 2013 Menggunakan Kontrol Annex : Studi Kasus Data Center Pt . Xyz the Development of Information Security Management System Implementation Based on Iso 27001 : 2013 Using a,” *e-Proceeding Eng.*, vol. 8, no. 2, pp. 2813–2825, 2021.

[8] A. Renaldy *et al.*, “Peran Sistem Informasi dan Teknologi Informasi Terhadap Peningkatan Keamanan Informasi Perusahaan,” *J. Ilmu Multidisplin*, vol. 2, no. 1, pp. 15–22, 2023, doi: 10.38035/jim.v2i1.212.

[9] M. S. Ummah, "Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dan ISO/IEC 27002 Pada Kantor Jasa Marga", vol. 11, no. 1. 2019. [Online]. Available: http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_Sistem_Pembetungan_Terpusat_Strategi_Melestari

[10] W. Apriandari and A. Sasongko, “Analisis Sistem Manajemen Keamanan Informasi Menggunakan Sni Iso/Iec 27001:2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus: Di Diskominfo Kota Sukabumi),” *J. Ilm. SANTIKA*, vol. 8, no. 1, pp. 715–729, 2018, [Online]. Available: www.tecnoid.id

[11] S. R. Musyarofah and R. Bisma, “Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001:2013 pada institusi pemerintah,” *Teknologi*, vol. 11, no. 1, pp. 1–15, 2021, doi: 10.26594/teknologi.v11i1.2152.

[12] M. Utomo, A. Holil, N. Ali, and I. Affandi, “900-5781-1-Pb,” vol. 1, no. 1, pp. 2–7, 2012.

[13] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, “Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022,” *J. SAINTEKOM*, vol. 14, no. 1, pp. 84–94, 2024, doi: 10.33020/saintekom.v14i1.623.

[14] Y. S. Dharmawan, R. A. W. Yani, and A. M. Putri, “Penyusunan Dokumen SOP Sistem Manajemen Keamanan Aset Informasi Dinas Pariwisata Kebudayaan Pemuda dan Olahraga Kab. Sumenep Menggunakan Framework COBIT 5 dan ISO 27001:2013,” *Sisfo*, vol. 11, no. 02, 2024, doi: 10.24089/j.sisfo.2024.06.005.

[15] F. Mauladani, “Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan SNI ISO/IEC 27001 : 2013 dan SNI ISO/IEC 27005 : 2013 (Studi Kasus Direktorat Pengembangan Teknologi Dan Sistem Informasi),” vol. 2013, 2017.

[16] S. Rif and R. Bisma, “Pembuatan Standard Operating Procedure ( SOP ) Keamanan Informasi Berdasarkan Framework ISO / IEC 27001 : 2013 dan ISO / IEC 27002 : 2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun,” *JEISBI*

*(Journal Emerg. Inf. Syst. Bus. Intell.*, vol. 01, pp. 43–50, 2020.

[17] BSN, "Standar Nasional lndonesia (SNl) ISO/IEC 27001:2013," pp. 1–62, 2013.

[18] J. R. Woda and R. Bisma, "Pembuatan Dokumen Prosedur Keamanan Informasi Yang Mengacu Pada Cobit 5 dan ISO 27001 : 2013 Pada Badan Pengelola Keuangan Dan Aset Daerah Jawa Timur," *JEISBI Vol. 01 Nomor 01, 2020 (Journal Emerg. Inf. Syst. Bus. Intell. Pembuatan*, vol. 01, pp. 51–59, 2020.

[19] A. M. Amrullah, Y. Citriadin, and M. Thohri, "Manajemen Penggunaan Teknologi Informasi Dan Komunikasi Dalam Meningkatkan Kinerja Guru Pendidikan Agama Islam Di Smkn 1 Narmada Kabupaten Lombok Barat," *J. Ilm. Mandala Educ.*, vol. 9, no. 3, pp. 2176–2181, 2023, doi: 10.58258/jime.v9i3.5897.

[20] Diah Ayu Saraswati *et al.*, "Analisis Kegiatan P5 di SMA Negeri 4 Kota Tangerang sebagai Penerapan Pembelajaran Terdiferensiasi pada Kurikulum Merdeka," *J. Pendidik. Mipa*, vol. 12, no. 2, pp. 185–191, 2022, doi: 10.37630/jpm.v12i2.578.

[21] D. S. Sinaga, P. N. S. Siregar, J. Sinaga, M. Siregar, and M. Pasaribu, "Analisis Strategi Pemilihan Narasumber Webinar terhadap Peningkatan Jumlah Member pada PT. Dilo Medan," *Remik*, vol. VII, no. 1, p. 855, 2023, [Online]. Available: https://www.jurnal.polgan.ac.id/index.php/remik/article/view/12155/1423

[22] M. Hendayun, A. Zulianto, S. Sekolah, and T. Ilmu, "Audit Keamanan Sistem Informasi Akademik Stikes Jenderal Achmad Yani Menggunakan SNI ISO / IEC 27001 : 2013 Abstraksi Pendahuluan," *ISSN 2548-8082 / E-ISSN 2615-6350 Vol.3 No.2 Ed. 2019 J u r n a l P R O D U K T I F | 25 Audit*, vol. 3, no. 2, pp. 25–35, 2019.

[23] Nandang Firmansyah, Regi Refian Garis, and Asep Nurdin Rosihan Anwar, "Implementasi Kebijakan Tata Kelola Keamanan Informasi Dan Jaringan Oleh Dinas Komunikasi Dan Informatika Kabupaten Ciamis," *J. Educ. Gov. Wiyata*, vol. 1, no. 3, pp. 143–154, 2023, doi: 10.71128/e-gov.v1i3.13.