JURNAL ILMU KOMPUTER
Volume 2 Nomor 2, Desember, 2024
ISSN: 3031-125X (ONLINE)
Penerbit: Program Studi Teknik Informatika S-2 Universitas Pamulang

# Analisis Dan Implementasi Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001 (Studi Kasus Pada PT.XYZ)

Rizki Septiyanto Wibowo[1], Tukiyat[2], Sajarwo Anggai[3],Winarni[4]

[(1,3)] Teknik Informatika, S-2, Universitas Pamulang, Tangerang Selatan, Banten, Universitas Pamulang

[2)] Badan Riset dan Inovasi Nasional, Indonesia

Email: [1]riskiwibowo153@gmail.com , [2]tukiyat@brin.go.id , [3]sajarwo@gmail.com, [4]dosen02874@unpam.ac.id

***ABSTRACT***

*It has become a current necessity in every company regarding the implementation of information and communication technology governance in efforts to improve service quality. The implementation of information and communication technology governance is a critical factor in enhancing service quality across various companies. Therefore, the adoption of an Information Security Management System (ISMS) based on the ISO 27001:2013 standard becomes essential, in line with the conduct of regular audits to ensure its effectiveness. This research aims to develop and design an information security governance framework in accordance with ISO/IEC 27001 and to conduct audits on the system that has been implemented in PT. XYZ, to ensure its compliance with good and efficient standards. The methodology used is Plan-Do- Check-Act (PDCA), with data collection techniques through interviews and distribution of questionnaires for internal audits. The research findings indicate that the average ISO/IEC 27001 maturity level is at levels three and four. It is expected that this research can assist and provide recommendations related to security controlsused as guidelines and procedures for the implementation of information security, as well as ensuring the overall operation runs in accordance with ISO 27001 standards.*

*Keywords: Audit, ISO/IEC 270001, Information Security Management System (SMKI), Plan-Do-Check-Act (PDCA).*

**ABSTRAK**

Sudah menjadi kebutuhan saat ini di setiap perusahan mengenai penerapan tata kelolateknologi informasi dan komunikasi dalam upaya peningkatan kualitas layanan. Implementasi tata kelola teknologi informasi dan komunikasi merupakan faktor penting dalam meningkatkan kualitas layanan di berbagai perusahaan. Oleh karena itu, penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar ISO 27001:2013 menjadi esensial, sejalan dengan pelaksanaan audit berkala untuk menjamin efektivitasnya. Penelitian ini bertujuan untuk mengembangkan dan merancang kerangka tata kelola keamanan informasi yang sesuai dengan ISO/IEC 27001 dan melaksanakan audit terhadap sistem yang telah diterapkan di PT.XYZ, guna memastikan penerapannya sesuai dengan standar yang baik dan efisien. Metodologi yang digunakan adalah Plan-Do-Check-Act (PDCA), dengan teknik pengumpulan data melalui wawancara dan distribusi kuesioner untuk audit internal. Hasil penelitian menunjukkan bahwa nilai maturity level ISO/IEC 27001 rata rata berada di level tiga dan empat, diharapkan hasil penelitian ini dapat membantu dan memberikan rekomendasi terkait dengan kontrol keamanan yang digunakan sebagai pedoman dan prosedur penerapan keamanan informasi, serta memastikan keseluruhan operasional berjalan sesuai dengan standar ISO 27001.

Kata Kunci : Audit, ISO/IEC 270001, Sistem Manajemen Keamanan Informasi (SMKI), Plan-Do- Check-Act (PDCA).

## 1. PENDAHULUAN

Dalam era digital yang semakin maju seperti saat ini, informasi menjadi salah satu aset yang paling penting bagi organisasi. Informasi dapat berupa data karyawan, data pelanggan, data keuangan, dan informasi lainnya yang sangat rahasia dan bernilai tinggi.Keamanan informasi menjadi sangat penting karena jika terjadi kebocoran atau kerusakanpada informasi tersebut, dapat berdampak buruk pada organisasi, termasuk kerugian finansial, reputasi yang rusak, dan hilangnya kepercayaan dari pelanggan dan mitra bisnis.

PT. XYZ adalah perusahaan yang bergerak di bidang industri keuangan berbasis teknologi yang berkembang pesat di era digital saat ini. PT XYZ menyediakan layanan pinjaman berbasis teknologi yang memanfaatkan data dan analisis untuk memudahkan proses pengajuan dan pencairan pinjaman bagi nasabah. Perusahaan fintech lending dapat memberikan solusi keuangan yang lebih cepat, mudah, dan terjangkau dibandingkan dengan institusi keuangan tradisional sehingga sangat penting memiliki sistemmanajemen keamanan informasi yang efektif dan memenuhi standar.

ISO 27001:2013 merupakan dokumen standar sistem manajemen keamanan informasi (SMKI), sering kali digunakan oleh perusahaan untuk menerapkan keamanan sistem informasi, dengan menerapkan standar ISO 27001:2013 perusahaan dapat melindungi, memelihara kerahasiaan, integritas dan ketersediaan informasi serta untuk mengelola dan mengendalikan risiko keamanan informasi pada organisasi perusahaan. Dalam penelitian ini penerapan yang dipakai untuk manajemen keamanan informasi PT.XYZ adalah ISO 27001:2013.

Berdasarkan penelitian Heru Susanto et al yang berjudul Information Security Management System Standards: A Comparative Study Of The Big Five, menerangkan bahwa informasi adalah aset organisasi di era modern saat ini dan penting untuk melindungi asset tersebut. Namun tidak ada yang dapat menjamin seratus persen (100%) keamanan dari informasi. Penelitian ini menghasilkan perbandingan standar keamanan informasi menggunakan ISO 27001, BS 7799, PCIDSS, ITIL dan COBIT yang dilihat dari sisi penempatan dan kekhususan penggunaan setiap standar dan negara yang menggunakannya.

Penelitian yang dilakukan oleh Georg Disterer dengan judul ISO/IEC 27000, 27001 and 27002 for Information Security Management, mengemukakan pentingnya mengukurkekuatan dari keamanan informasi, yang merupakan salah satu inisiatif terpenting dari manajemen information technology (IT). Standar keamanan informasi dapat digunakan untuk mengembangkan dan memelihara kekuatan sistem manajemen keamanan informasi. Standar ISO/IEC 27000, 27001, dan 27002 merupakan standar yang telah diterima dan diadaptasi. Perusahaan yang menggunakan standar ISO/IEC 27001 diberikan sertifikat ISMS/SMKI oleh pihak ketiga yang telah mengukur keamanan dan bukti yang ada.

Penelitian oleh Anirban Sengupta yang berjudul Modeling Dependencies of ISO/IEC27002:2013 Security Controls, menerangkan bahwa kontrol keamanan seperti kebijakan, prosedur, hukum dan regulasi atau alat keamanan dan teknik-tekniknya membantudalam mitigasi risiko terkait sistem informasi perusahaan. Kontrol dari ISO/IEC 27002:2013 merupakan inter-dependent dan terdiri dari beberapa aspek yang berbeda pada pengimplementasiannya. Kurang tepatnya penggunaan kontrol merupakan salah satu kendala yang sulit ditangani oleh perusahaan. Penelitian ini menyajikan analisis kontrol pada ISO/IEC 27001:2013.

Perbedaan penelitian yang sudah dilakukan oleh peneliti terdahulu dengan yang dilakukan ini adalah pada penelitian ini berfokus mengaudit manajemen keamanan informasi di PT XYZ menggunakan ISO 27001:2013. Dengan kajian ini tentu akan diketahui apakah semua klausul dan annex yang terdapat dalam ISO 27001:2013 sudah di implementasikan dengan baik atau belum dalam satu tahun terakhir. Kemudian selanjutnya diberikan rekomendasi untuk klausul dan annex yang belum terimplementasi dengan prosedur yang ada didalam PT XYZ. Unsur kebaruan dan kontribusi didalam penelitian ini adalah Audit Sistem Manajemen Keamanan Informasi pada perusahaan tersebut menggunakan ISO 27001:2013, olehkarena itu dengan penelitian ini diharapkan dapat memberikan kontribusi berupa rekomendasi- rekomendasi berdasarkan standar ISO 27001:2013.

### 1.1. Analisis Sistem Informasi

Analisis sistem merupakan suatu konsep yang akan dirancang oleh satu atau sekelompok orang. Analisis itu mengidentifikasi, menyatakan, merencanakan, menyusun

dan merancang masalah-masalah dalam suatu objek atau sistem. Tahapan kerja dari analisis sistem sebagai berikut (Winda & Ashwin 2018).

### 1.2. Sistem Manajemen Keamanan Informasi

Keamanan Informasi adalah suatu proses penjagaan informasi dari keseluruhan ancaman yang mungkin bisa saja terjadi dalam upaya untuk memastikan dan menjamin kelangsungan bisnis, meminimalisasi resiko bisnis serta memaksimalkan ataupun mempercepat pengembalian investasi serta peluang bisnis. Keamanan sistem informasi merupakan suatu bentuk kegiatan perlindungan atau pencegahan terhadap gangguan penyalahgunaan informasi yang dilakukan oleh orang yang tidak bertanggung jawab terhadap jalannya suatu sistem (Eri, Dkk 2023).

### 1.3. ISO/IEC 27001:2013

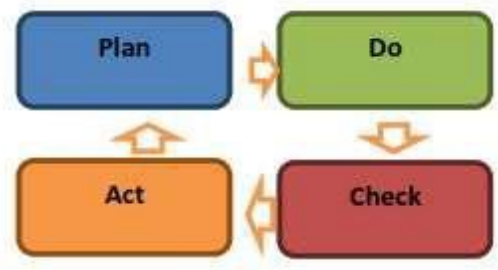
Standard ISO 27001:2013 merupakan suatu revisi dari standard sebelumnya yaitu standard ISO 27001:2005. ISO 27001:2013 tetap bisa diadopsi oleh suatu organisasi sebagaimana versi-versi yang terdahulu. Sistem Manajemen Keamanan Informasi ISO 27001:2013 telah ditetapkan oleh Badan Standarisasi Nasional Nomor 61/KEP/BSN/4/2016 serta Peraturan Menteri Kominfo Nomor 4 tahun 2016Pasal 7. Dalam ISO 27001:2013 terdapat 14 area pengamanan informasi yaitu kebijakan keamanan informasi, keamanan sumber daya manusia, manajemenasset, mengakses kontrol dan mengelola akses pengguna, teknologi kriptografi, keamanan fisik, keamanan operasional, mengamankan komunikasi dan transfer data, kkuisisi,pengembangan, dan dukungan sistem informasi yang aman, keamanan untuk pemasok dan pihak ketiga, manajemen Insiden, kesinambungan bisnis/pemulihan bencana, dan kepatuhan (Eri Dkk, 2023).

ISO 27001:2013 merupakan suatu standar diterbitkan oleh lembaga International Organization for Standardization (ISO) dan International Electrotechnical Commision (IEC). Sebuah standar Internasional dalam penerapanSMKI atau Security Management Systems (ISMS), menjadi salah satu best praktis didalam penerapan keamanan informasi (Eri, Dkk 2022).

## 2. METODE

Pada penelitian ini menggunakan metode *Plan-Do- Check-Act* (PDCA), metode digunakan sebagai jaminan kualitas dan persyaratan dalam ISMS ISO 27001 Sistem Manajemen Keamanan Informasi, selain itu proses digunakan juga sebagai alat dalam

proses audit internal agar organisasi memahami proses dan persyaratan ISO 27001 sebelum menghadapi proses sertifikasi oleh Lembaga Eksternal, siklus PDCA ISO 27001 akan memberikan gambaran penerapan tata Kelola dan kesesuaian dengan tujuan perusahaan.




Gambar 3. 1 Siklus PDCA

Kerangka kerja ISO 27001 telah berkembang pesat dan dinilai sebagai praktik terbaik untuk mendapatkan sertifikat yang diakui internasional. Seperti penjelasan sebelumnya untuk mengimplementasikan ISO 27001 siklus PDCA terlebih dahulu digunakan dalam proses internet audit. Siklus ini akan membantu organisasi mengidentifikasi isu-isu internal dan eksternal yang merupakan ancaman dan risiko bagi organisasi.

Pada proses PDCA terlihat dilakukan secara berkelanjutan atau tidak berhenti pada suatu proses. Siklus proses PDCA yang berkelanjutan adalah salah satu kunci yang disediakan kerangka acuan ISO/IEC 27001 untuk membantu setiap organisasi dalam memastikan adanya adaptasi ke perubahan baru secara konsisten terhadap lingkup ancaman.

## 2.1. Tahap Perencanaan *(Plan)*

Metode penelitian yang dipergunakan oleh peneliti menggunakan Studi literatur dilakukan dengan mencari dan mempelajari teori-teori yang berkaitan terhadap penelitian sejenis yang pernah dilakukan sebelumnya atauteori-teori tersebut berasal dari buku, jurnal, ebook yang mendukung penelitian ini serta untuk mengetahui teknik-teknik dan metode yang akan digunakan dalam pengumpulan data, pengolahan data dan penyelesaian permasalahan yang ada. Pencarian referensi yang dilakukan nantinya dapat menunjang dalam pengerjaan sistem manajemen keamanan informasi pada PT. XYZ

### 2.2. Tahap *DO*

Proses ini akan sangat membantu organisasi menerapkan prosedur ISMS ISO 27001 dan menghindari hambatan yang mungkin muncul. Do (Pelaksanaan) fase ini adalah tahap dimana organisasi melakukan implementasi Sistem Manajemen Keamanan Informasi (ISMS) yang telah ditetapkan sebelumnya, yaitu kebijakan, kontrol, proses, dan prosedur SMKI.

### 2.3. Tahapan Evaluasi (*Check*)

Mengukur kinerja proses yang tidak sesuai dengan kebijakan, objek dan laporan praktis SMKI untuk menghasilkan review manajemen. Pada tahapan ini dilakukan pengecekan, pengawasan serta audit untuk mengetahui apakah semua sudah sesuai dengan rencana sebelumnya, apabila ada kendala maka harus segera dilakukan evaluasi dan memperbaiki kesalahan yang terjadi.

### 2.4. Tahapan Tindak Lanjut (*Act*)

Setelah evaluasi, tahap selanjutnya adalah pembaruan dan peningkatan SMKI. Pada tahap ini organisasi harus melakukan audit sertifikasi dan rencana tindak lanjut. Tahap act adalah tahap untuk mengambil tindakan yang seperlunya terhadaphasil- hasil dari tahap check.

## 3. HASIL DAN PEMBAHASAN

### 3.1. Hasil Perbandingan *Framework* NIST CSF dan ISO 27001

Seperti yang dinyatakan oleh (Hendi, Dkk 2021) keuntungan yang dimiliki oleh framework NIST adalah sebagian besar kategori dan subkategori menggunakan referensi dari kerangka kerja framework lain seperti ISO 27001 dan COBIT. Framework NIST juga menerapkan konsep profile untuk evaluasi keamanan secara keseluruhan. Profile kerangka kerja merepresentasikan penyesuaian dan prioritas kegiatan dan hasil untuk berbagai industri dan organisasi sesuai dengan kebutuhan mereka. ISO 27001 adalah standar framework information security yang diterbitkan pada tahun 2013 dan merupakan revisi dari ISO 27001:2009. Framework tersebut menerapkan prinsip-prinsip dasar Information Security Management Systems PDCA (*Plan-Do-Check-Act*) dan ISO 27001 merupakan salah satu standar framework yang paling terkenal karenatidak hanya diterapkan di organisasi Amerika Serikat, tetapi di seluruh dunia.

Tabel 4.1 Perbandingan Framework NIST CSF dan ISO 27001

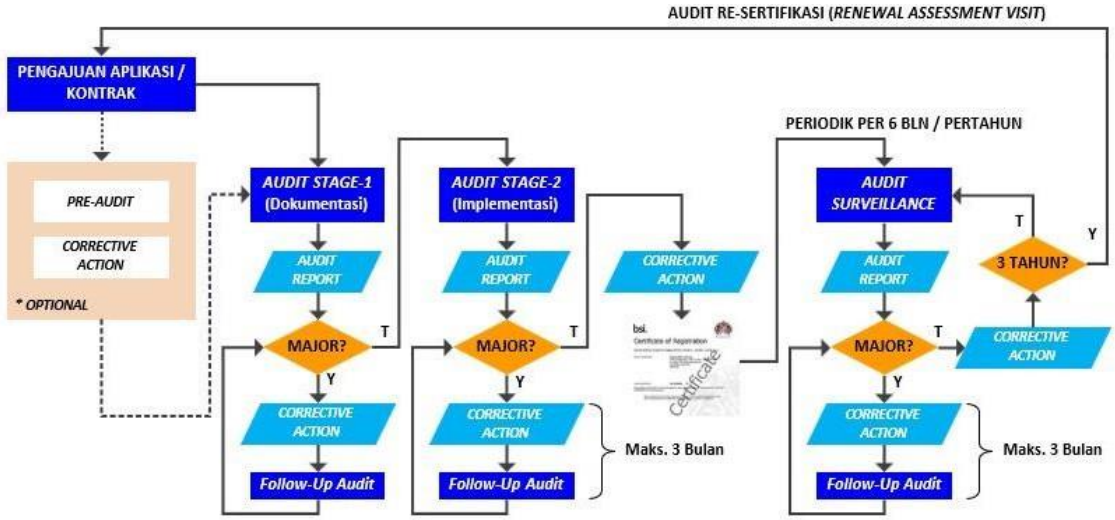
| Area | NIST CSF | ISO 27001 |
|---|---|---|
| *Function* | *Information Security Framework* | *Information Security Framework* |
| *Basis* | *Risk Management* | *Risk Management* |
| *Cerfitiable* | *No* | *Yes* |
| *Scope* | *Optional guidelines, best practices and standards for implementing and improving cybersecurity programs.* | *Information security standard that describes how to implementan ISMS (Information Security Management System).* |
| *Structure* | *Core divided into 5 function, 23 categories and 108 subcategiries.* | *Consist 7 section od PDCA, 14 clase and 133 control.* |

Pada tabel 4.1 di jelaskan bahwa NIST CSF dan ISO 27001 memiliki fungsi yang sama yaitu fokus terhadap keamanan informasi dan berbasis manajemen risiko. Perbedaan dari kedua framework tersebut adalah bahwa penerapan NIST CSF tidak memiliki sertifikasi untuk perusahaan yang menerapkannya, sedangkan ISO 27001 memiliki sertifikasi yang dapat menyatakan bahwa perusahaan tersebut telah menerapkan standarnya secara efektif. Cakupan dari NIST CSF berupa sebuah panduan opsional, praktik terbaik untuk standar penerapan dan peningkatan program keamanan siber, sedangkan cakupan ISO 27001 berupa Standar keamanan informasi yang menjelaskan bagaimana mengimplementasikan ISMS (*Information Security Management System*). NIST CSF terdiri atas 5 fungsi inti, 23 kategori dan 108 sub kategori yang diperlukan untuk pelaksanaan dalam audit sistem informasisedangkan ISO 27001 mencakup total 7 proses opsional dalam PDCA (Plan-Do- Check-Act),14 klausa dan 133 kontrol.

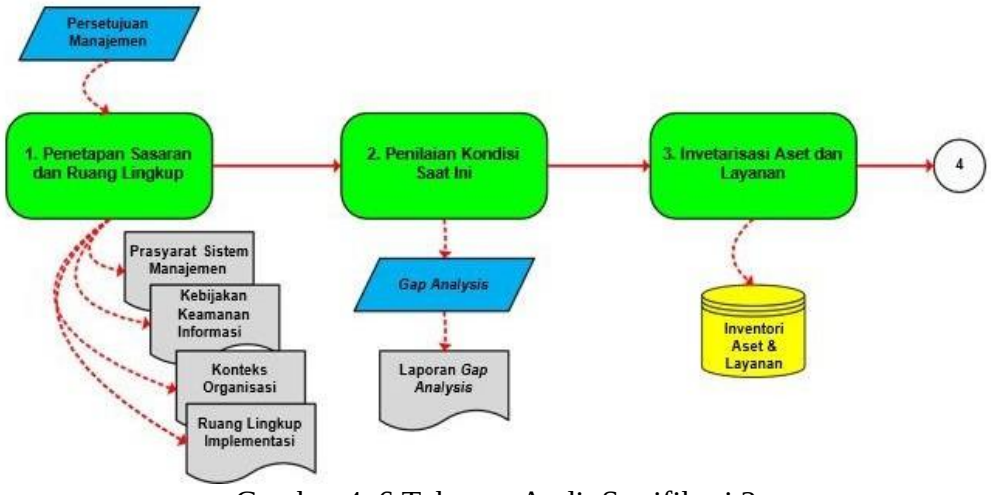
Menurut (Hendi Dkk, 2021) dengan adanya manajemen keamanan informasi yang baik, diharapkan perusahaan ataupun organisasi yang menerapkannya dapat menghadapi risiko-risiko yang muncul akibat penyalahgunaan data ataupun serangan cybersecurity lainnya. Standar ISO 27001 merupakan standar yang sangat ideal untuk diterapkan dalam manajemen keamanan informasi di sebuah organisasi/perusahaan, karena standar tersebut menyediakan sertifikasi yang dapat menyatakan bahwa organisasi/perusahaan tersebut telah menerapkan standar keamanan informasi yang efektif. Sedangkan, standar NIST

CSF lebih baik dalam hal penataan area keamanan yang akan diimplementasikan melalui konsep profile keamanan yang ingin dicapai.

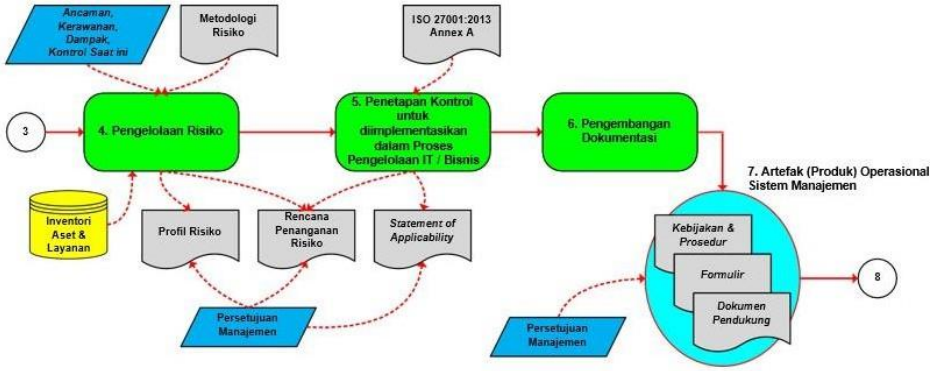
Tahapan Audit sertifikasi ISO 27001 adalah langkah penting untuk memastikan bahwa organisasi memiliki sistem manajemen keamanan informasi yang kuat dan efektif. Dengan mendapatkan sertifikasi ISO 27001, organisasi dapat meningkatkan kepercayaan pelanggan, melindungi aset informasi, dan mencapai keunggulan kompetitif, berikut adalah gambar dari tahapan proses audit sertifikasi dan tahapan implementasi menuju SMKI.



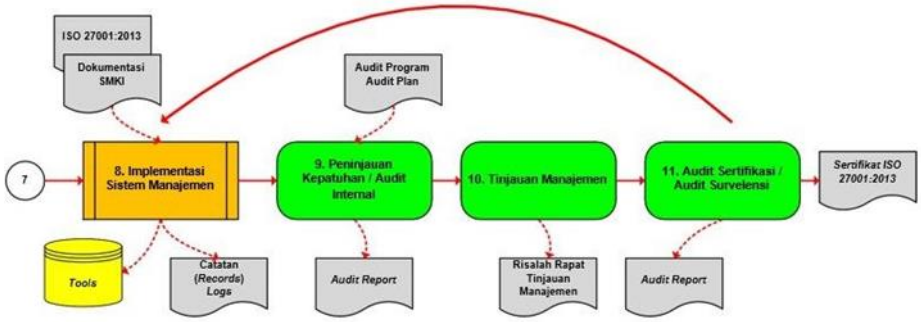

Gambar 4. 5 Tahapan Audit Sertifikasi 1




Gambar 4. 6 Tahapan Audit Sertifikasi 2




Gambar 4. 7 Tahapan Implementasi Menuju SMKI




Gambar 4. 8 Tahapan Implementasi Menuju SMKI

### 3.2. Implementasi ISO 27001:2013 pada PT Anugerah Digital Indonesia

1. CONTEXT OF THE ORGANIZATION

Konteks Organisasi dalam ISO 27001 merujuk pada pemahaman yang mendalam tentang faktor-faktor internal dan eksternal yang dapat mempengaruhi kemampuan organisasi untuk mencapai tujuan dalam mengelola keamanan informasi. Ini adalah langkah awal yang sangat penting dalam implementasi Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO 27001.

2. LEADERSHIP

Leadership berperan penting dalam memastikan keberhasilan penerapan Sistem Manajemen Keamanan Informasi (SMKI). ISO 27001 menekankan bahwa manajemen puncak (top management) memiliki tanggung jawab besar untuk menetapkan arahan strategis dan memastikan bahwa keamanan informasi menjadi prioritas organisasi. Berikut adalah beberapa poin penting terkait leadership dalam ISO 27001 misalnya komitemen dari manajemen puncak, kebijakan keamanan informasi dan peran, tanggung jawab, dan wewenang organisasi..

3. PLANNING

Tahap perencanaan yang memastikan bahwa Sistem Manajemen Keamanan Informasi (SMKI) direncanakan secara efektif agar dapat memenuhi persyaratan keamanan informasi yang telah ditetapkan. Proses ini mencakup beberapa elemen penting yaitu general, identifikasi risiko keamanan informasi, perlakuan risiko keamanan informasi dan Information security objectives and planning to achieve them.

4. SUPPORT

Mengacu pada elemen-elemen yang diperlukan untuk memastikan bahwa Sistem Manajemen Keamanan Informasi (SMKI) dapat beroperasi secara efektif dan sesuai dengan standar. Bagian support ini mencakup berbagai aspek seperti sumber daya, kompetensi, kesadaran, komunikasi, serta dokumentasi dan informasi terdokumentasi yang diperlukan untuk mendukung penerapan SMKI..

5. OPERATION

Kegiatan dan proses yang diperlukan untuk mengimplementasikan, memelihara, dan mengelola Sistem Manajemen Keamanan Informasi (SMKI) secara efektif. Beberapa aspek penting dalam operation adalah operational planning and control, Information security risk assessment dan Information security risk treatment.

6. PERFORMANCE EVALUATION

Tujuan dari evaluasi kinerja ini adalah untuk memastikan bahwa sistem manajemen keamanan informasi berjalan dengan efektif dan sesuai dengan kebijakan, tujuan, dan persyaratan keamanan yang telah ditetapkan. Bagian performance evaluation termasuk monitoring, measurement, analysis and evaluation, internal audit, dan management review.

7. IMPROVEMENT

Improvement (perbaikan) merujuk pada proses berkelanjutan untuk meningkatkan efektivitas Sistem Manajemen Keamanan Informasi (SMKI) yang diterapkan oleh organisasi. ISO 27001 menekankan pentingnya perbaikan terus- menerus untuk memastikan bahwa keamanan informasi tetap relevan, efektif, dan sesuai dengan perkembangan risiko serta perubahan dalam lingkungan organisasi.

8. ANNEX A (A.5)

Tujuan dari kontrol ini adalah untuk memastikan adanya arahan yang jelas dan dukungan terhadap keamanan informasi. Hal ini dicapai dengan mendefinisikan

kebijakan keamanan informasi yang selaras dengan tujuan strategis organisasi dan memastikan kebijakan tersebut ditinjau secara berkala agar tetap relevan dan efektif.

9. ANNEX A (A.6)

Bagian yang membahas pengendalian akses fisik dan lingkungan, misalnya pengendalian akses fisik terhadap asset, lingkungan yang aman, pengelolaan area aman dan control pengunjung.

10. ANNEX A (A.7)

Mengacu pada lampiran dari standar yang memberikan panduan terkait kontrol keamanan informasi, khususnya dalam manajemen sumber daya manusia. ISO 27001 adalah standar internasional untuk sistem manajemen keamanan informasi (SMKI). Annex 7 lebih rinci dalam memberikan kontrol untuk memastikan bahwa karyawan, kontraktor, dan pihak ketiga yang memiliki akses ke informasi organisasi, dipilih, dilatih, dan dikelola dengan baik guna mencegah pelanggaran keamanan.

11. ANNEX A (A.8)

Annex A.8 ini berkaitan dengan pengelolaan aset informasi. Annex ini memberikan panduan mengenai kontrol yang perlu diterapkan untuk melindungi aset informasi, baik yang bersifat fisik maupun digital, dari ancaman keamanan. Aset di sini mencakup data, perangkat keras, perangkat lunak, sumber daya manusia, serta hal-hal lainnya yang penting untuk operasional organisasi.

12. ANNEX A (A.9)

Berkaitan dengan kontrol akses (Access Control). Kontrol akses merupakan elemen penting dalam sistem manajemen keamanan informasi, karena bertujuan untuk memastikan bahwa hanya individu yang berwenang yang memiliki akses ke informasi dan sumber daya perusahaan, sesuai dengan kebutuhannya.

13. ANNEX A (A.10)

Annex A.10 ini berhubungan dengan pengelolaan komunikasi dan operasi sistem informasi. Bagian ini memberikan panduan tentang kontrol yang diperlukan untuk memastikan bahwa informasi dan sumber daya teknologi informasi diproses dengan aman, serta bagaimana organisasi harus mengelola operasionalnya secara aman untuk melindungi integritas dan kerahasiaan data.

14. ANNEX A (A.11)

Berhubungan dengan Kontrol Akses (Access Control). Tujuan dari Annex ini adalah untuk membatasi akses ke informasi hanya kepada individu yang berwenang, guna melindungi integritas, kerahasiaan, dan ketersediaan informasi dalam organisasi.

15. ANNEX A (A.12)

Berkaitan dengan keamanan operasi (Operational Security). Bagian ini fokus pada langkah-langkah yang perlu diambil oleh organisasi untuk memastikan bahwa operasi teknologi informasi dan komunikasi (TIK) berjalan dengan aman. Ini mencakup berbagai kontrol yang dirancang untuk melindungi sistem, layanan, dan data dari ancaman yang mungkin muncul selama operasi sehari-hari. Bisa dilihat pada lampiran 20.

16. ANNEX A (A.13)

Annex 13 dalam konteks ini berkaitan dengan “Kepatuhan” atau “Compliance”. Lampiran ini memberikan pedoman mengenai kontrol dan prosedur yang perlu diterapkan untuk memastikan bahwa organisasi mematuhi semua persyaratan hukum, regulasi, dan peraturan yang relevan terkait keamanan informasi.

17. ANNEX A (A.14)

Berkaitan dengan keamanan dalam pengembangan dan pemeliharaan sistem. Lampiran ini memberikan pedoman tentang bagaimana organisasi harus menangani keamanan informasi dalam seluruh siklus hidup pengembangan sistem, mulai dari tahap perencanaan hingga implementasi dan pemeliharaan.

18. ANNEX A (A.15)

Mengacu pada kontrol akses dan penanganan data yang berkaitan dengan pengelolaan akses informasi dan pengendalian yang tepat terhadap data untuk menjaga keamanan informasi dalam organisasi.

19. ANNEX A (A.16)

Berkaitan dengan pengelolaan pemulihan dan kontinuitas operasional. Meskipun standar ini tidak secara eksplisit mencantumkan Annex 16 dalam dokumennya, prinsip-prinsip yang relevan sering kali dibahas dalam konteks kontrol dan panduan untuk menjaga kelangsungan bisnis.

20. ANNEX A (A.17)

Berfokus pada kontrol keamanan informasi yang berkaitan dengan aspek keamanan fisik dan lingkungan. Meskipun dalam standar ISO 27001:2013, tidak terdapat

Annex 17 yang spesifik, tapi pada lampiran ini merujuk kepada bagian dari kontrol terkait dalam Annex A yang menyentuh pada topik tersebut.

21. ANNEX A (A.18)

Berfokus pada kontrol keamanan informasi dalam hubungan dengan pihak ketiga. Lampiran ini memberikan panduan tentang cara organisasi harus mengelola risiko yang terkait dengan interaksi dengan pihak ketiga yang memiliki akses ke informasi dan sistem informasi organisasi.

Tabel 4.2 ISO 270001 Summary

| ISOIEC 27001 | ISOIEC 27001 Audit | *% Compliance* |
|---|---|---|
| 27001-001 | *Context of the organisation* | **100** |
| 27001-002 | *Leadership* | **100** |
| 27001-003 | *Planning* | **100** |
| 27001-004 | *Support* | **100** |
| 27001-005 | *Operation* | **100** |
| 27001-006 | *Performance evaluation* | **100** |
| 27001-007 | *Improvement* | **100** |
| 27001-008 | Annex A (A.5) | **100** |
| 27001-009 | Annex A (A.6) | **100** |
| 27001-010 | Annex A (A.7) | **100** |
| 27001-011 | Annex A (A.8) | **100** |
| 27001-012 | Annex A (A.9) | **100** |
| 27001-013 | Annex A (A.10) | **100** |
| 27001-014 | Annex A (A.11) | **100** |
| 27001-015 | Annex A (A.12) | **100** |
| 27001-016 | Annex A (A.13) | **100** |
| 27001-017 | Annex A (A.14) | **100** |
| 27001-018 | Annex A (A.15) | **100** |
| 27001-019 | Annex A (A.16) | **100** |
| 27001-020 | Annex A (A.17) | **100** |
| 27001-021 | Annex A (A.18) | **100** |

Tabel 4.3 Maturity Level

| ***Annex*** | ***Current Maturity Level*** | **Standar *Maturiry* Level ISO/IEC** | **PT ADI *Maturity* Target** |
|---|---|---|---|
| *A.5 Information Security Policy* | 5 | 5 | 5 |
| *A.6 Information Security Organization* | 5 | 5 | 5 |
| *A.7 Human Resource Security* | 5 | 5 | 5 |
| *A.9 Access Control* | 4,92 | 5 | 4 |
| *A.10 Cryptography* | 5 | 5 | 4 |
| *A.12 Operation Security* | 5 | 5 | 4 |

| | | | |
|---|---|---|---|
| *A.13 Communication Security* | 5 | 5 | 4 |
| *A.14 Acquisition, Development and Maintenance of Systems* | 4,9 | 5 | 4 |
| *A.16 Information Security Incident Management,* | 5 | 5 | 5 |
| *A.18 compliance* | 5 | 5 | 4 |
| ***Average*** | **5,0** | **5,0** | **4,4** |

## 4. KESIMPULAN

Berdasarkan hasil dan pembahasan yang telah dibahas dapat disimpulkan bahwa laporan dari hasil analisis dapat digunakan untuk mencapai standar sistem manajamen keamanan informasi (SMKI) dengan menggunakan ISO/IEC 27001 dan ISO/IEC 27002 sebagai rekomendasi dan peningkatan keamanan informasi. Berikut adalah hasil dari penelitian ini dengan menggunakan metode *Plan, Do, Check, Act* :

a. Keamanan informasi menjadi salah satu kebutuhan utama bagi perusahaan, terutama untuk menjaga kerahasiaan, integritas, dan ketersediaan data penting. PT. XYZ sebagai perusahaan di bidang fintech lending membutuhkan sistem manajemen keamanan informasi yang efektif sesuai standar internasional ISO/IEC 27001:2013 untuk mengurangi risiko keamanan siber, meningkatkan kepercayaan pelanggan, dan mematuhi regulasi.
b. Dalam penelitian ini, metode Plan-Do-Check-Act (PDCA) digunakan sebagai pendekatan untuk menerapkan dan mengevaluasi SMKI. Data dikumpulkan melalui wawancara dan kuesioner audit internal untuk memahami kondisi keamanan informasi di PT. XYZ. Audit internal menunjukkan bahwa tingkat kematangan penerapan SMKI pada PT. XYZ berada pada level 2 dan 3, menunjukan Organisasi memiliki kebijakan dan prosedur yang tertulis, tetapi belum diimplementasikan secara penuh pada PT XYZ setelah dilakukan analisis dan implementasi, hasil nilai maturity menunjukan berada pada level 4 dan 5 yang dimana sudah memenuhi standar yang ditentukan ISO.

## DAFTAR PUSTAKA

[1] Anggi A, Oky & Ike. (2016) Perencanaan Dan Implementasi Information Security Management System Menggunakan Framework ISO/IEC 20071. Diakses dari Perencanaan dan Implementasi Information Security Management

System Menggunakan Framework ISO/IEC 20071 | Putra | *Jurnal Teknologi dan Sistem Komputer* (undip.ac.id)

[2] Bakri Muhammad & Nia Irmayana. (2017) Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi SIMHPBPKPMenggunakan Standar ISO 27001. Diakses dari ANALISIS DAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI SIMHP BPKP MENGGUNAKAN STANDAR ISO 27001 | Bakri | *Jurnal Tekno Kompak* (teknokrat.ac.id)

[3] Budiarto Raden. (2017). Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode FMEA Dan ISO 27001 Pada Organisasi XYZ. Diakses dari Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung, Lampung: Information Security Audit | POSITIF : *Jurnal Sistem dan Teknologi Informasi* (poliban.ac.id)

[4] Ciptaningrum Dkk (2015). Audit Keamanan Sistem Informasi pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5. Seminar NasionalTeknologi Informasi dan Komunikasi. Yogyakarta.

[5] Chalifa (2015) STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005. Diakses dari 04_STANDAR_MANAJEMEN_KEAMANAN_SISTEM_INFORMASI_BERBASIS_ISO_27001-libre.pdf (d1wqtxts1xzle7.cloudfront.net)

[6] Desy Dwi Prasetyowati Dkk. (2019). Evaluasi Manajemen Keamanan Informasi MenggunakanIndeks KAMI Berdasarkan ISO/IEC 27001:2013 pad Politeknik Ilmu Pelayaran Semarang . Diakses dari Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang | Prasetyowati | JOINS (*Journal of Information System*) (dinus.ac.id)

[7] Edy Soesanto Dkk. (2023). Sistem Manajemen Keamanan Informasi dengan StandarISO/IEC 27001 dan ISO/IEC 27002 pada PT Jasa Marga. Diakses dari Sistem manajemen keamanan informasi dengan standar ISO/IEC 27001 dan ISO/ICE 27002 pada PT Jasa Marga | Co-Creation : *Jurnal Ilmiah Ekonomi Manajemen Akuntansi dan Bisnis* (arkainstitute.co.id)

[8] Eri Riana, Meiva & Octa. (2022) Analisis Maturity Level Dan Pdca Dalam Penerapan Proses Audit SMKI (Information Security Management System)

Menggunakan ISO 27001:2013 Pada PT Indonesia Game. Diakses dari 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) (seminar- id.com).

[9] Eri Riana, Meiva & Octa. (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. Diakses dari Diakses dari 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) (seminar-id.com)

[10] Erny, Rokhman & Ryan Adhitya. (2020). Perancangan Manajemen Keamananan Informasi Menggunkan Metode Analisis Risiko Iso 27005:2008 Pada Dinas Komunikasi Dan Informatika Jawa Barat. Diakses dari Perancangan Manajemen Keamanan Informasi Menggunakan Metode Analisis Risiko Iso 27005:2008 Pada Dinas Komunikasi Dan Informatika Provinsi Jawa Barat | Nursetyawati | eProceedings of Engineering (telkomuniversity.ac.id)

[11] Fadzri, Suprapto & Andi. (2019). Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten). Diakses dari Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten) | *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* (ub.ac.id)

[12] Firzah, Hanim & Bekti. (2017). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. Diakses dari Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC

27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya - Neliti

[13] Faza, Widhyi & Admajai (2020). Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur). Diakses dari Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur) | *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* (ub.ac.id)

[14] Fitroh, Dkk. (2017) Pentingnya Implementasi ISO 27001 Dalam Manajemen Keamanan : Sistematika Review. Diakses dari PENTINGNYA IMPLEMENTASI ISO 27001 DALAM MANAJEMEN KEAMANAN : SISTEMATIKA REVIEW | Fitroh | Prosiding Semnastek (umj.ac.id)

[15] Gustiana A.P & Yudi Priyadi. (2019). Rekomendasi Pemodelan Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001:2013 dan DFDpada PT. XYZ. Diakses dari View of Rekomendasi Pemodelan Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001:2013 dan DFD pada PT. XYZ (stikom- bali.ac.id)

[16] Hatomo Arif. (2019) Perencanaan Strategis Sistem Informasi Dan Sistem Manajemen Keamanan Informasi Berbasis ISO / IEC 27001: 2013 Menggunakan Ward & Peppard Pada Perusahaan Transshipment. Diakses dari yusrian,+5604-24798-3- ED (2).pdf

[17] Hartati Tuti. (2017). Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013. Diakses dari Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001: 2013 | KOPERTIP : *Scientific Journal of Informatics Management and Computer* (kopertipindonesia.or.id)

[18] Hartati, Gema & Citra. (2023). Sistem Manajemen Keamanan Informasi Perlindungan Nilai Matakuliah berbasis ISO 27001. Diakses dari Sistem Manajemen Keamanan Informasi Perlindungan Nilai Matakuliah berbasis ISO 27001 | *Jurnal ICT: Information Communication & Technology* (ikmi.ac.id)

[19] Hilaluddin Jauhary Dkk. (2022). Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi: Literatur Review. Diakses dari

Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi : Literatur Review| Jauhary | Media Jurnal Informatika (unsur.ac.id)

[20] Hariyanto, Bambang. (2004). Sistem Manajemen Basis Data. Bandung: Informatika

[21] Ibra & Rahardian. (2021). Perancangan Sistem Informasi Manajemen Risiko

[22] berdasarkan ISO 27001:201 (Sistem Manajemen Keamanan Informasi). Diakses dari Perancangan Sistem Informasi Manajemen Risiko berdasarkan ISO 27001:2013 (Sistem Manajemen Keamanan Informasi) | Journal of Emerging Information System and Business Intelligence (JEISBI) (unesa.ac.id)

[23] Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto). Diakses dari Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto) | Sholikhatin | *Jurnal Ilmiah IT CIDA* (amikomsolo.ac.id)

[24] Kadir, A. (2003). Pengenalan Sistem Informasi. Yogyakarta: ANDI.

[25] Lestari, Putri. (2018). Skripsi Analisis Faktor-Faktor yang Mempengaruhi Kepercayaan dalam Bertransaksi Online Shopping pada MahasiswaUIN Syarif Hidayatullah Jakarta.

[26] Mardi & Jajasukma. (2018). Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan InformasiSNI ISO/IEC 27001. Diakses dari Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001 | PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic (unismabekasi.ac.id).

[27] Mei, Wing & Armadyah. (2017). Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 Dan Cobit 5. Diakses dari Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 Dan Cobit 5 | Lenawati | SPEED - Sentra Penelitian Engineering dan Edukasi

[28] Nasher Fuad. (2018). Perancangan Sistem Manajemen Keamanan Informasi Layanan Pengadaan Barang/Jasa Secara Elektronik (LPSE) Di Dinas Komunikasi Dan Informatika Kabupaten CianjurDengan Menggunakan SNI ISO/IEC 27001:2013. Diakses dari Microsoft Word - mji pa fuad.docx (semanticscholar.org).

[29] Pangky Februari & Fitria (2019). Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung Lampung. Diakses dari Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung, Lampung: Information Security Audit | POSITIF : *Jurnal Sistem dan Teknologi Informasi* (poliban.ac.id)

[30] Rahmat Dadan. (2019). Perencanaan Sistem Manajemen Keamanan InformasiMenggunakan Standar SNI ISO/IEC 27001: 2013. Diakses dari Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar Sni Iso/Iec 27001: 2013 | COMPUTING | *Jurnal Informatika* (unibba.ac.id)

[31] Ritzkal, Arief & Hendri Hendrawan. (2016). Implementasi ISO/IEC 27001:2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) Pada Fakultas Teknik Uika-Bogor. Diakses dari IMPLEMENTASI ISO/IEC 27001:2013 UNTUK SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) PADA FAKULTAS TEKNIK UIKA-BOGOR | Ritzkal | Prosiding Semnastek (umj.ac.id)

[32] Rizki & Bambang. (2021). Evaluasi Manajemen Keamanan Informasi MenggunakanIndeks Keamanan Informasi (KAMI) Pada Jaringan (Studi Kasus : UIN Sunan Kalijaga Yogyakarta). Diakses dari Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta) | Jurnal Teknologi Informasi dan Ilmu Komputer (ub.ac.id)

[33] Siti, Arief & Emha. (2018). Analisis Keamanan Sistem Informasi Dengan ISO 27001(Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto). Diakses dari Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto) | Sholikhatin | Jurnal Ilmiah IT CIDA (amikomsolo.ac.id)

[34] Sitta & Rahadian. (2021). Analisis Kesenjangan Sistem Manajemen Keamanan Informasi (SMKI) Sebagai Persiapan Sertifikasi ISO/IEC 27001:2013 Pada Institusi Pemerintah. Diakses dari Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001:2013 pada institusi pemerintah | Teknologi: *Jurnal Ilmiah Sistem Informasi* (unipdu.ac.id)

[35] Satori D & Komariah A (2013). Metode Penelitian Kualitatif. Bandung. Alfabeta

[36] Sofyanti. (2014). *Skripsi* Rancang Bangun Sistem Informasi Penerimaan KaryawanBerbasis WEB (Studi Kasus: PT Desalite Esbang Jaya). Jakarta: Universitas Islam Negeri Syarif Hidayatullah

[37] Sarno & Iffano. (2009). Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press. Sheikhpour & Modiri. (2012). A Best Practice Approach for Integration of ITIL and ISO/IEC 27001 Services for Information Security Management.Indian journal of science and technology, Vol. 5, No. 2.

[38] Tripton & Krause. (2011). Information Security Management Handbook, Volume 5, 6th Edition. Boca Raton: CRC Press

[39] Wenceslaus & Fahmy. (2020). Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI)ISO/IEC 27001:2013. Diakses dari Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013 | Pamungkas | Jurnal Sistem Komputer dan Informatika (JSON) (stmik-budidarma.ac.id)

[40] Winda & Ashwin Sasongko (2018). Analisis Sistem Manajemen Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus: Di Diskominfo Kota Sukabumi). Diakses dari 391-Article Text-834-1-10-20190322 (4).pdf