ULIL ALBAB : Jurnal Ilmiah Multidisiplin
Vol.3, No.6, Mei 2024

Sistem Manajemen Keamanan Informasi (SMKI) di PT. Surveyor Indonesia Cabang Surabaya: Penerapan Standar ISO 27001:2013

R. Teddy Adiyanto Prawiranata
Universitas Katolik Widya Mandala
E-mail: managemaster.r.teddy.22@ukwms.ac.id

Article History:
Received: 30 April 2024
Revised: 08 Mei 2024
Accepted: 10 Mei 2024

Keywords: *Information Security Management System (ISMS), ISO 27001:2013*

Abstract: *This article discusses the implementation of the Information Security Management System (ISMS) and the adoption of the ISO 27001:2013 standard at PT Surveyor Indonesia Surabaya Branch. The purpose of writing this article is to analyze the process of designing, implementing, and maintaining the IMS, as well as the integration of the ISO 27001:2013 standard in the company's business practices. The results of the article show that the implementation of the SMKI and the adoption of the ISO 27001:2013 standard have had a positive impact on improving the information security and overall performance of PT Surveyor Indonesia Surabaya Branch. However, there were some challenges and barriers faced during the implementation process, such as limited resources and resistance from employees. Nonetheless, the integration of ISO 27001:2013 standard in PT Surveyor Indonesia Surabaya Branch is not only formal compliance but also implemented in daily business practices to protect the company's critical information and ensure optimal information security. The writing of this article is expected to make a significant contribution to PT Surveyor Indonesia, the academic community, and information security practitioners, as well as being a valuable contribution in the context of implementing the ISO 27001:2013 standard in an increasingly connected business era.*

PENDAHULUAN

Keamanan informasi merupakan aspek yang tidak dapat diabaikan dalam menjalankan operasi perusahaan modern, terutama mengingat dominasi teknologi informasi pada saat ini. PT. Surveyor Indonesia, perusahaan yang bergerak dalam bidang jasa survei dan konsultasi telah mengambil langkah strategis dengan menerapkan Sistem Manajemen Keamanan Informasi (SMKI), terutama di unit bisnisnya di Surabaya, dengan mengacu pada standar internasional ISO27001:2013. Paper ini bertujuan untuk melakukan analisis mendalam terhadap implementasi SMKI di PT. Surveyor Indonesia Cabang Surabaya, dengan tujuan mengeksplorasi proses perancangan, pelaksanaan, dan pemeliharaan SMKI, serta integrasi standar ISO27001:2013 dalam praktik bisnis perusahaan tersebut. Harapannya, penulisan artikel ini akan mengungkap praktik terbaik dan tantangan yang dihadapi dalam adopsi standar tersebut, sekaligus menyoroti

dampaknya terhadap keamanan informasi dan kinerja keseluruhan PT. Surveyor Indonesia. Pemahaman yang diperoleh dari penulisan artikel ini diharapkan akan memberikan kontribusi signifikan bagi PT. Surveyor Indonesia, komunitas akademis, dan praktisi keamanan informasi, serta menjadi sumbangan berharga dalam konteks penerapan standar ISO27001:2013 di era bisnis yang semakin terhubung.

LANDASAN TEORI

Informasi

Secara Etimologi, Kata informasi ini berasal dari kata Bahasa Perancis kuno informacion (tahun 1387) mengambil istilah dari bahasa Latin yaitu informationem yang berarti "konsep, ide atau garis besar". Informasi ini merupakan kata benda dari informare yang berarti aktivitas. Aktifitas dalam "pengetahuan yang dikomunikasikan". Pengertian informasi menurut para ahli:

1. Abdul Kadir dan McFadden dkk.(1999) mendefinisikan informasi sebagai data yang telah diproses sedemikian rupa sehingga meningkatkan pengetahuan seseorang yang menggunakan data tersebut.
2. Jogiyanto dalam bukunya yang berjudul Analisis dan Desain Sistem Informasi, berpendapat bahwa informasi adalah data yang diolah menjadi bentuk yang lebih berguna bagi yang menerimanya.

Ciri-Ciri Informasi yang berkualitas, yaitu :

1. Informasi harus Relevan, yang artinya informasi tersebut mempunyai manfaat oleh pemakainya.
2. Informasi harus Akurat, yang artinya informasi harus bebas dari kesalahan-kesalahan dan harus jelas mencerminkan maksudnya.
3. Tepat pada waktunya, yang artinya informasi yang diterima tidak boleh terlambat.
4. Konsisten, yang artinya informasi yang diterima sesuai dengan datanya tidak mengalami perubahan yang tidak benar.

Keamanan Informasi

Definisi Keamanan informasi :

1. Keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. (G. J. Simons)
2. *"A computer is secure if you can depend on it and its software to behave as you expect."* (Garfinkel & Spafford)

Jadi keamanan informasi merupakan suatu usaha untuk melindungi informasi melalui beberapa jenis media seperti komputer, mesin fax dan juga fasilitas pendukung penyimpanan data dan informasi seperti media dokumen *hardcopy* dari penyalahgunaan oleh orang yang tidak mempunyai hak akses. Keamanan informasi dapat juga diartikan sebagai upaya melindungi, mengamankan aset informasi dari ancaman yang mungkin terjadi sehingga dapat membahayakan bagi aset informasi tersebut. Tujuan keamanan informasi untuk mencapai tiga sasaran utama, yaitu:

1. Confidentiality {Kerahasiaan) : melindungi data dan informasi perusahaan dari penyingkapan orang –orang yang tidak berhak.
2. Integrity (Integritas) : sistem informasi perlu menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan.
3. Availability (Ketersediaan) : meyakinkan bahwa data dan informasi perusahaan hanya dapat digunakan oleh orang yang berhak menggunakannya.

Manajemen Keamanan Informasi

Manajemen Keamanan Informasi mempunyai empat tahapan yaitu:

1. Identifikasi *threats (ancaman)*. Menyerang sumber daya informasi perusahaan.Yang termasuk dalam ancaman keamanan informasi adalah organisasi, mekanisme, personal atau peristiwa yang dapat berpotensi menimbulkan kejahatan pada sumber daya informasi perusahaan. Ancaman dapat berasal dari internal atau external, baik itu disengaja atau tidak disengaja.
2. Mendefinisikan resiko dari ancaman. Tindakan tidak sah yang menyebabkan resiko dapat digolongkan ke dalam empat jenis:
   a. Pencurian dan Penyingkapan tidak sah,
   b. Penggunaan tidak sah,
   c. Pengrusakan dan Penolakan layanan yang tidak sah,
   d. Modifikasi yang tidak sah.
3. Penetapan kebijakan keamanan informasi. Tanpa melihat apakah perusahaan mengikuti manajemen resiko atau strategi pelaksanaan brenchmark, kebijakan keamanan harus diimplementasikan untuk mengarahkan keseluruhan program.
4. Menerapkan kontrol yang tertuju pada resiko. Kontrol adalah mekanisme yang diimplementasikan baik untuk melindungi perusahaan dari resiko atau untuk memperkecil dampak resiko terhadap perusahaan.

ISO 27001:2013

ISO 27001 adalah suatu standar internasional untuk Information Security Manajemen System (ISMS). ISO 27001 berlaku untuk semua bisnis. Keamanan informasi yang dimiliki dalam bentuk apapun, bukan hanya berupa data elektronik.

Di Uni Eropa diperkirakan kejahatan internet dan serangan cyber meningkat pesat dalam beberapa tahun terakhir. Yang jadi sasaran bukan hanya perusahaan swasta, melainkan juga lembaga pemerintahan. Perbedaan atau Perubahan ISO 27001: 2013 dengan ISO 27001: 2005:

1. ISO 27001: 2013 memiliki 114 kendali (kontrol) dalam 14 kelompok domain,
2. ISO 27001: 2005 memiliki 133 kendali (kontrol) dalam 11 kelompok domain.

Adanya perubahan beberapa kontrol pada ISO 27001:2013 ini adalah salah satu dampak dari adanya perubahan/perkembangan teknologi. Untuk lebih jelasnya tentang ISO 27001: 2013.

Gambar 1. Perbedaan ISO/IEC 27001: 2005 dengan ISO/IEC 27001: 2013

Adanya perubahan beberapa kontrol pada ISO 27001:2013 ini adalah salah satu dampak dari adanya perubahan/perkembangan teknologi. Untuk lebih jelasnya tentang ISO 27001: 2013 dapat dilihat sebagai berikut:

1. *Scope of the standard*
2. *How the document is referenced*
3. *Reuse of the terms and definitions in ISO/IEC 27000*
4. *Organizational context and stakeholders*
5. *Information security leadership and high-level support for policy*
6. *Planning an information security management system;risk assessment; risk treatment*
7. *Supporting an information security management system*
8. *Making an information security management system operational*
9. *Reviewing the system's performance*
10. *Corrective action*

Berdasarkan Establish ISMS 27001: 2013 di mana urutan ke 4 adalah *Contex of Organization* yang dapat di uraikan pada gambar 2.

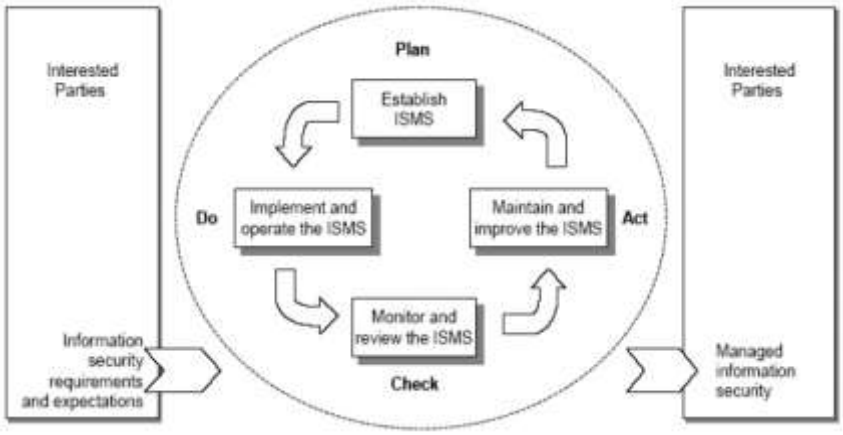
ISO 27001: 2013 Standard
Documentation, Implementation and Audit Requirements classified

Clause	Description	Documentation Requirements	Implementation Requirements	Audit Requirements
4	Context of the organization			
4.1	Understanding the organization and its context	'About the Organization' in the IS Policy document	Understand the organization, its nature of business and defining it in the IS Policy document.	Review the IS Policy document
4.2	Understanding the needs and expectations of interested parties	'Target Audience' in the IS Policy document	Brainstorming with Management and including it in the IS Policy document.	Review the IS Policy document
4.3	Determining the scope of the ISMS	'ISMS Scope' in the IS Policy document	Brainstorming with Management and including it in the IS Policy document.	Review the IS Policy document
4.4	ISMS	The IS Policy document	• Establishment of IS • Appointment of IS Manager • Conducting IS Trainings and Awareness • Defining RACI	Review the IS Policy document

Gambar 2. ISO 27001: 2013 *Standard Documentation, Implementation and Audit Requirment Classified*

Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) adalah suatu bentuk susunan proses yang dibuat berdasarkan pendekatan resiko bisnis untuk merencanakan (*Plan*), mengimplementasikan dan mengoperasikan (*Do*), memonitoring dan meninjau (*Check*), serta memelihara dan meningkatkan atau mengembangkan (*Act*) terhadap keamanan informasi perusahaan. Sistem Manajemen Keamanan Informasi (SMKI), Biasanya dapat digunakan para manajer untuk mengukur, memonitor dan mengendalikan keamanan informasi.



Gambar 3. PDCA yang diterapkan untuk proses SMKI (Sistem ManajemenKeamanan Informasi)

Sistem Manajemen Keamanan Informasi memberikan perlindungan informasi dan penghitungan aset yang ada. Terdapat tiga komponen kunci dalam menyediakan jaminan layanan keamanan informasi, diantaranya:

1. *Confidentiality* (Kerahasiaan) ketika data hanya boleh diakses oleh yang berwenang.
2. *Integrity* (Integritas) ketika informasi tidak boleh berubah (*tampered, altered, modifield*) oleh pihak yang tidak berhak.
3. *Availability* (Ketersediaan) ketika informasi harus tersedia ketika dibutuhkan.

METODE PENELITIAN

Penulis menggunakan teknik analisis deskriptif kualitatif, menjelaskan suatu temuan penelitian dengan menggunakan data dari berbagai sumber referensi. Bagian dari studi literatur melibatkan pengorganisasian sumber penelitian, membaca dan mencatat, dan menggunakan metode pengumpulan data perpustakaan. Jenis data yang digunakan adalah data sekunder, yang bersumber dari berbagai sumber terpercaya, antara lain buku, jurnal, artikel, web, dan sumber lainnya.

HASIL DAN PEMBAHASAN

Implementasi SMKI pada PT. Surveyor Indonesia Cabang Surabaya

PT. Surveyor Indonesia Cabang Surabaya telah secara teliti merancang, melaksanakan, dan memelihara Sistem Manajemen Keamanan Informasi (SMKI) mereka. Proses perencanaan SMKI ini mencakup acuan terhadap Standar Operasional Prosedur (SOP) Security TI di PT Surveyor Indonesia, serta merujuk pada beragam standar seperti SNI ISO 9001:2015, PP 50 tahun 2012, SNI ISO/IEC 17020:2012, SNI ISO/IEC 17025:2008, SNI ISO 14001:2015, OHSAS 18001:2007, Peraturan Kapolri No. 24 tahun 2007, Undang-Undang Republik Indonesia Nomor 19 Tahun 2016, dan SNI ISO 27001:2013. Implementasi kontrol keamanan tercermin dalam berbagai prosedur, termasuk manajemen media penyimpanan yang tidak terpakai, pemasangan antivirus, konfigurasi server, jaringan komputer, dan keamanan PC. Di samping itu, pengelolaan risiko tercermin dalam kegiatan seperti pencadangan data di server, pencadangan data secara berkala, serta pengaturan ruang server yang dilengkapi dengan sistem pengawasan tertutup (CCTV), perangkat pengatur suhu, dan Uninterrupted Power Supply (UPS) untuk menjaga kestabilan dan keamanan ruang

server. Dengan memperhatikan proses perencanaan, implementasi kontrol keamanan, dan pengelolaan risiko sesuai dengan standar dan prosedur terinci yang disediakan, PT. Surveyor Indonesia Cabang Surabaya telah berhasil mengimplementasikan SMKI dengan cermat.

Integrasi Standar ISO 27001:2013

Standar ISO 27001:2013 merupakah standar internasional yang mengatur manajemen keamanan informasi, memberikan kerangka kerja yang komprehensif untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi penting dalam suatu organisasi. Di PT. Surveyor Indonesia Cabang Surabaya, integrasi standar ISO 27001:2013 dilakukan dengan sungguh-sungguh dan berdasarkan struktur yang terencana. Peran manajemen senior sangat penting dalam memastikan kepatuhan terhadap standar ini. Mereka memiliki tanggung jawab utama dalam pembentukan kebijakan keamanan informasi yang sesuai dengan persyaratan standar ISO 27001:2013, serta memonitor dan memastikan implementasi kontrol keamanan yang sesuai dengan standar tersebut.

PT. Surveyor Indonesia Cabang Surabaya menerapkan praktik-praktik tertentu untuk memastikan keamanan informasi, seperti penerapan kebijakan pengelolaan password yang ketat, kebijakan penggunaan media penyimpanan yang tidak aktif, dan pelaksanaan pencadangan data secara berkala. Selain itu, perusahaan juga memiliki prosedur untuk menangani pemutusan hak akses jaringan bagi karyawan yang tidak lagi bekerja di perusahaan, serta memastikan bahwa setiap PC dilengkapi dengan perangkat lunak antivirus yang terpasang dan diperbarui secara teratur.

Dengan demikian, integrasi standar ISO 27001:2013 di PT. Surveyor Indonesia Cabang Surabaya tidak hanya merupakan komitmen formal semata, tetapi juga tercermin dalam praktik bisnis sehari-hari untuk menjaga keamanan informasi yang vital bagi perusahaan, sehingga memastikan tingkat keamanan informasi yang optimal.

Tantangan dan Hambatan

Selama proses implementasi Sistem Manajemen Keamanan Informasi (SMKI), PT. Surveyor Indonesia Cabang Surabaya menghadapi sejumlah tantangan dan hambatan yang perlu diatasi. Salah satu tantangan yang signifikan adalah keterbatasan sumber daya, terutama dalam konteks infrastruktur teknologi informasi yang diperlukan untuk mendukung implementasi SMKI. Meskipun perusahaan memiliki prosedur keamanan TI yang ketat, implementasi SMKI membutuhkan investasi tambahan dalam infrastruktur teknologi informasi untuk memastikan kepatuhan terhadap standar dan persyaratan yang ditetapkan.

Selain itu, hambatan organisasional juga merupakan faktor yang perlu diperhatikan selama proses implementasi SMKI. Ini dapat meliputi resistensi dari karyawan terhadap perubahan dalam prosedur keamanan TI yang sudah ada, serta adaptasi terhadap kebijakan dan prosedur baru yang diperlukan untuk mematuhi standar SMKI. Oleh karena itu, manajemen perlu memastikan adanya komunikasi yang efektif dan pelatihan yang memadai untuk memastikan bahwa seluruh karyawan memahami dan mendukung implementasi SMKI.

Meskipun PT. Surveyor Indonesia Cabang Surabaya telah memiliki prosedur keamanan TI yang komprehensif, tantangan terkait keterbatasan sumber daya dan resistensi dari karyawan menyoroti pentingnya adopsi strategi manajemen yang efektif untuk mengatasi hambatan tersebut selama proses implementasi SMKI.

Dampak Implementasi SMKI

Implementasi Sistem Manajemen Keamanan Informasi (SMKI) dan adopsi standar ISO 27001:2013 telah memberikan dampak yang signifikan terhadap keamanan informasi dan kinerja

PT. Surveyor Indonesia cabang surabaya. Dengan adanya SMKI, PT. Surveyor Indonesia cabang surabaya telah meningkatkan keamanan data secara keseluruhan. Hal ini terbukti dari pelaksanaan backup data di server yang dilakukan oleh Divisi TI sesuai dengan tingkat prioritas dan kepentingannya, serta pengujian hasil backup secara berkala untuk memastikan data hasil backup tidak rusak atau hilang. Selain itu, penggunaan server yang ditempatkan di ruang khusus yang tertutup secara fisik dan selalu dalam keadaan terkunci juga merupakan langkah penting dalam meningkatkan keamanan data.

Adopsi standar ISO 27001:2013 juga telah mengurangi risiko keamanan informasi dengan memberikan pedoman yang jelas dalam mengelola keamanan informasi. Hal ini tercermin dari kebijakan yang diterapkan, seperti pengaturan antivirus yang selalu diupdate, pembatasan akses ke server, dan pengelolaan password email dan aplikasi. Selain itu, kepercayaan dari pelanggan dan mitra bisnis juga meningkat karena perusahaan telah mematuhi standar internasional dalam mengelola keamanan informasi, sehingga memberikan keyakinan bahwa data mereka akan dijaga dengan baik.

Secara keseluruhan, implementasi SMKI dan adopsi standar ISO 27001:2013 telah membawa dampak positif dalam meningkatkan keamanan informasi dan kinerja PT. Surveyor Indonesia cabang surabaya secara menyeluruh.

KESIMPULAN

Implementasi Sistem Manajemen Keamanan Informasi (SMKI) dan adopsi standar ISO 27001:2013 telah membawa dampak positif dalam meningkatkan keamanan informasi dan kinerja PT. Surveyor Indonesia Cabang Surabaya secara menyeluruh. Dampak tersebut meliputi peningkatan keamanan data secara keseluruhan, pengurangan risiko keamanan informasi, peningkatan kepercayaan dari pelanggan dan mitra bisnis, serta adopsi praktik-praktik keamanan informasi yang ketat. Selain itu, dokumen juga menyoroti beberapa tantangan dan hambatan yang dihadapi selama proses implementasi SMKI, seperti keterbatasan sumber daya dan resistensi dari karyawan. Namun, integrasi standar ISO 27001:2013 di PT. Surveyor Indonesia Cabang Surabaya tidak hanya menjadi kepatuhan formal, tetapi juga diimplementasikan dalam praktik bisnis sehari-hari untuk melindungi informasi penting perusahaan dan memastikan keamanan informasi yang optimal.

Saran yang dapat diberikan adalah untuk memperhatikan keamanan informasi dengan serius, terutama dalam hal implementasi Sistem Manajemen Keamanan Informasi (SMKI) dan adopsi standar ISO 27001:2013. Hal ini termasuk dalam prosedur-prosedur seperti pengelolaan media penyimpanan yang tidak digunakan, instalasi antivirus, pengaturan server, jaringan komputer, keamanan PC, serta pelaksanaan backup data secara berkala. Selain itu, perusahaan juga perlu memperhatikan prosedur pemutusan hak akses jaringan bagi karyawan yang tidak bekerja lagi di perusahaan, serta penggunaan anti virus yang terpasang dan selalu diperbarui di setiap PC. Agar di jadikan pertimbangan di kemudian hari oleh PT. Surveyor Indonesia,terutama cabang surabaya untuk update ke ISO 27001:2022. Organisasi yang saat ini tersertifikasi ISO 27001:2013 akan memiliki waktu tiga tahun untuk bertransisi ke ISO/IEC 27001:2022. Periode transisi dimulai pada 31 Oktober 2022, dan berakhir pada 31 Oktober 2025. Sertifikasi berdasarkan ISO 27001:2013 akan kedaluwarsa atau dicabut pada akhir masa transisi.

DAFTAR REFERENSI

A. Kadir, Pengenalan Sistem Informasi, Yogyakarta: Andi Offset, 2003.
A. Kristanto, Komputer dan Teknologi Informasi, Yogyakarta: Graha Ilmu, 2003.

Agustian, Fajrin. 2011. Kajian Tingkat bendaharaan dan Anggaran Negara (SPAN) Kematangan Sistem Manajemen KeamananInformasi menggunakan Indeks KAMI (Studi Kasus: Kantor Pusat Direktorat Jenderal Pajak). Sekolah Tinggi Akuntansi Negara.

Badan Standardisasi Nasional. 2009. SNIISO/IEC 27001:2009 Teknologi Informasi –Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan. Jakarta: Badan Standardisasi Nasional – BSN.

Catur Daya Solusi, "Upgrading ISO 27001:2005 ke ISO 27001:2013," 9 Maret 2015. [Online]. Available: http://caturdayasolusi.com/upgrading-iso-270012005-ke-iso- 270012013/.

H. M. Jogiyanto, Analisis dan desain sistem informasi, Yogyakarta: Andi Offset, 2005.

Hartati, T. (2017). Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013.

Kementerian Komunikasi dan Informatika. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Jakarta: Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi dan Informatika Informasi Kementerian Komunikasi dan Informatika.

Prosedur Security TI nomor dokumen : P-DTI-02

Syarif, R. A., & Nugroho, A. (2016). Analisis Tingkat Kematangan Sistem Manajemen Keamanan Informasi Direktorat Jenderal Perbendaharaan Diukur dengan Menggunakan Indeks Keamanan Informasi (Studi Kasus: Aplikasi SPAN).