IMPLEMENTASI

SMKI – ISO 27001:2022

Konsultan Implementasi SMKI

Rahadian Consulting didukung oleh tim ahli yang berpengalaman dan memiliki sertifikat ISO 27001 untuk implementasi. Konsultan ini akan membantu mulai dari tahap awal sampai organisasi memiliki sertifikat ISO 27001, bahkan mendukung kegiatan surveillance tahunan agar memastikan dapat mempertahankan sertifikat ISO 27001.

PPTI
Perkumpulan Profesional Teknologi Informasi

Rahadian Consulting

TAHAPAN IMPLEMENTASI SISTEM MANAJEMEN KEAMANAN INFORMASI

FAKTOR KEBERHASILAN

TIM KONSULTAN

STRATEGI

RAHADIAN CONSULTING
021 - 25033662 / 02518579009
info@rahadian-consulting.com

www.rahadian-consulting.com

2023

Tahapan Implementasi ISO 27001:2022

Tahapan implementasi terdiri dari:

Perkiraan Durasi implementasi jika menggunakan konsultn untuk kedua fase (Plan dan Do) terutama bergantung pada ukuran organisasi:

- ✓ Perusahaan dengan jumlah hingga 20 karyawan - hingga 3 bulan
- ✓ 20 hingga 50 karyawan – 3 hingga 5 bulan
- ✓ 50 hingga 200 karyawan – 5 hingga 8 bulan
- ✓ Lebih dari 200 karyawan – 8 hingga 20 bulan

Peran dalam proyek implementasi:

ISO 27001 tidak mengharuskan perusahaan membentuk tim proyek, tetapi ini akan membantu perusahaan dengan 200 karyawan atau lebih; untuk perusahaan kecil, cukup hanya memiliki manajer proyek yang akan mengoordinasikan proyek dengan rekan kerja lainnya.

Implementasi ISO 27001:2022

Peran dalam proyek implementasi ISO 27001:2022 Rahadian Consulting			
Peran	**Jumlah Pegawai**		
	< 200	200 – 2.000	> 2.000
Manajer Proyek	1 hari per minggu	50 % dari total waktu proyek	100 % dari total waktu proyek
Security officer		50 % dari total waktu proyek	100 % dari total waktu proyek
Tim Proyek	Tidak wajib diperlukan	Kepala departemen adalah anggota tim proyek – 15 jam per setiap kepala departemen (di seluruh proyek)	Kepala departemen adalah anggota tim proyek – 30 jam per setiap kepala departemen (di seluruh proyek)
Kepala departemen	7 jam per setiap kepala departemen (di seluruh proyek)		
Manajemen Puncak	5 jam dari total waktu proyek	10 jam dari total waktu proyek	15 jam dari total waktu proyek

Upaya ini akan diperlukan jika perusahaan menggunakan alat ISO 27001 atau konsultan untuk membantu ; jika tidak, perusahaan akan membutuhkan lebih banyak usaha.

Pembiayaan dalam proyek implementasi:

Total biaya implementasi akan tergantung pada hal-hal berikut:

- ✓ Ukuran perusahaan, yaitu jumlah karyawan (harus menghitung hanya karyawan yang akan dimasukkan dalam ruang lingkup ISO 27001)
- ✓ Tingkat kekritisan informasi (misalnya, informasi di bank dianggap lebih kritis dan menuntut tingkat perlindungan yang lebih tinggi)
- ✓ Teknologi yang digunakan organisasi (misalnya, pusat data cenderung memiliki biaya lebih tinggi karena sistemnya yang rumit)
- ✓ Persyaratan undang-undang (biasanya, sektor keuangan dan pemerintah sangat diatur sehubungan dengan keamanan informasi)

Beberapa jenis biaya yang perlu perhitungkan:

- ✓ Biaya Pelatihan
- ✓ Biaya bantuan eksternal
- ✓ Biaya waktu karyawan
- ✓ Biaya teknologi baru
- ✓ Biaya sertifikasi

Faktor Keberhasilan Implementasi ISO 27001:2022

Beberapa faktor keberhasilan implementasi ISO 27001:2022 sebagai berikut:

- ***Dukungan Manajemen menjadi kewajiban***; Komitmen manajemen harus diutamakan – jika eksekutif puncak tidak melihat manfaat nyata dalam meningkatkan tingkat keamanan dengan menetapkan aturan yang jelas dan standar, sebaiknya perusahaan menginvestasikan untuk hal lain.
- ***Pengetahuan tentang ISO 27001;*** walaupun sudah menerapkan ISO 27001, individu terkait harus mempelajari cara melakukannya. Implementasi ISO 27001 terlalu rumit untuk dipahami hanya dengan membaca standarnya.
  Ada beberapa kursus ISO 27001 yang tersedia untuk pemula atau untuk pengguna tingkat lanjut
- ***Jalankan implementasi sebagi sebuah proyek;*** Jika tahu persis apa tujuannya, siapa yang bertanggung jawab atas apa, jika sumber daya tersedia, dan apa yang dapat disampaikan, tidak hanya akan mempercepat proses – tetapi juga meningkatkan peluang untuk mendapatkan hasil yang sukses.
  Contoh kegiatan proyek implementasi ISO 27001:2022

Tahapan Proyek	Tahapan Implementasi	Tugas	Dokumen yang digunakan	Status
INISIASI	Mendapatkan dukungan manajemen	Sampaikan manfaat kepada manajemen dan dapatkan komitmen mereka		
PLAN	Persiapkan proyek	Menulis prosedur untuk kontrol dokumen	00 – Prosedur Pengendalian Dokumen dan Catatan	
		Tulis rencana proyek termasuk definisi manajer proyek, tim proyek, sponsor proyek, sumber daya yang diperlukan, dan milestone	01 - Project Plan	
	Mengidentifikasi persyaratan	Tetapkan prosedur untuk mengidentifikasi pihak yang berkepentingan	02 - Prosedur Identifikasi Persyaratan	
		Mengidentifikasi kebutuhan pihak yang berkepentingan	02.1 - Daftar Persyaratan Hukum, Peraturan, Kontrak dan Lainnya	

- ***Pilih Manajer Proyek yang berpengalaman***; pilihlah orang dengan ciri-ciri sebagai berikut:
  - Pengetahuan yang baik tentang bisnis dan proses TI di perusahaan – orang ini tidak perlu ahli TI, tetapi orang ini harus memiliki pengetahuan tentang TI
  - Dia perlu memiliki cukup waktu untuk menjalankan proyek
  - Harus memiliki otoritas yang cukup untuk mendorong semua perubahan yang diperlukan

Rahadian Consulting

Tim Konsultan Implementasi ISO 27001:2022

Rahadian didukung dengan konsultan yang berpengalaman implementasi Sistem Manajemen Teknologi Informasi ISO 27001

A. Adang (Senior Konsultan)

Sertifikat yang dimiliki

- ✓ Lead Auditor ISO 27001: 2013, IRCA Certified.
- ✓ Lead Implementer ISO 27001:2013 BSI Certified.
- ✓ Auditor QMS ISO 9001:2015 BSI Certified .
- ✓ Auditor BCMS ISO 22301 & PASS 99, TUV Rheinland.
- ✓ Data Center, BSI (2020).

Pengalaman

- ✓ SO IT Service & Management Sub Direktorat ITSG (2016-2019).
- ✓ Off-1 IT Service Platform & Integration (ITSG) Telkom Indonesia (2010-2012).
- ✓ Asman OSS Regional-III Bandung Jawa Barat (2007- 2009).
- ✓ Asman Feasibility Analisys ISDC-III Bandung (2005-2007).
- ✓ Asman Perencanaan System ISDC-III Bandung. (2003-2006).
- ✓ Analisys Network & Infrastruktur ISDC-III Bandung (2001-2003).
- ✓ Spesialis Network Managemen Reg-III Bandung (2000-2001).
- ✓ Implemented & Acessor ISO 27001 for Kominfo Bandung City (2020-2021).
- ✓ Team Policy Maker ISMS ISO 27001 for Kementrian ATR/BPN (2020).
- ✓ Acessor ISMS Implemented for Peduli Lindungi Application Kemenlu (2020)
- ✓ Assessor ISO 27001 for Data Center Pusdatin Kominfo Wonosobo. (2020).
- ✓ Team Member Draft Policy Maker ISMS (SMKI) for Telkom Indonesia (2018-2019)
- ✓ Program Manager Sertification Consultant ISO 27001:2013 for Data Center Jiwasraya (2019-2020).
- ✓ Certification Consultant ISO 27001:2013 for T-Money Application (2017 -2019).
- ✓ Internal Auditor ISO 27001:2013 for Data Center New Centrix Telkom Indonesia (2016-2019).
- ✓ Internal Auditor ISO 27001, for IMS Telkom Indonesia (2012 - 2019).

B. Rangga (Senior Konsultan)

Sertifikat yang dimiliki

- ✓ IMPLEMENTASI ISO 27001:2013
- ✓ PENYUSUNAN DOKUMEN ISO 27001:2013
- ✓ SURVEILENCE ISO 27001:2013
- ✓ ASSESSMENT INTERNAL ISO 27001:2013

Pengalaman

- ✓ Implementasi ISO 27001:2013 - BSN
- ✓ Penyusunan Dokumen ISO 27001:2013 – BSN
- ✓ Surveilence ISO 27001:2013 – BSN
- ✓ Implementasi ISO 27001:2013 - BPPT
- ✓ Penyusunan Dokumen ISO 27001:2013 – BPPT
- ✓ Implementasi ISO 27001:2013 – Bank Mandiri
- ✓ Penyusunan Dokumen ISO 27001:2013 – Bank Mandiri
- ✓ Implementasi, penyusunan Dokumen, survelience diberbagi perusahaan Seperti Kereta Api Indonesia, Badan Informasi Geospatial (BIG), Kementrian Keuangan, Antam, ITSEC ASIA, Garuda Indonesia, XL AXIATA, PT. Terminal Peti Kemas – Surabaya

C. Dicky (Junior Konsultan)

Sertifikat yang dimiliki

- ✓ ISO 31000:2018 Introduction and Implementation (Risk Management)
- ✓ Information Security Management System – Introduction and Implementation ISO/IEC 27001:2013
- ✓ ISO/IEC 27001:2013 Internal Auditor
- ✓ ISO/IEC 27001:2022 Implementation
- ✓ ITF+ - IT Fundamental CompTIA

Pengalaman

- ✓ Manajemen Risiko SP4N LAPOR.go.id

Strategi Implementasi ISO 27001:2022

Ada 3 strategi implementasi ISO 27001:2022 yaitu:

A. Melaksanakan sendiri tanpa bantuan pihak luar

Karyawan perusahaan / organisasi melakukan semua pekerjaan tanpa menggunakan bantuan dari konsultan atau alat apa pun. Ini adalah pilihan terbaik jika organisasi tidak menginginkan orang luar di perusahaan dan jika anggaran sangat ketat, tetapi ini hanya layak jika memiliki karyawan yang sudah berpengalaman dalam ISO 27001

B. Melaksanakan sendiri dengan bantuan pihak luar

Organisasi menerapkan standar sendiri (dengan melakukan semua analisis, wawancara, menulis dokumentasi, dll.), tetapi menggunakan alat dan panduan ISO 27001 dari pakar eksternal untuk menyelesaikan proyek. Ini adalah opsi terbaik jika organisasi memiliki anggaran yang moderat, dan jika ingin karyawan mempelajari cara terbaik untuk mengelola keamanan.

C. Konsultan melakukan sebagian besar pekerjaan

Organisasi mempekerjakan seorang ahli dari luar (yaitu, konsultan ISO 27001) untuk melakukan seluruh pekerjaan – konsultan ini akan melakukan semua pekerjaan dan akan memberikan dokumentasi lengkap kepada organisasi. Ini biasanya merupakan opsi tercepat untuk menerapkan standar, tetapi juga yang paling mahal