ISO 2000/

Standar ISO 20000 adalah standar yang dipergunakan untuk sertifikasi manajemen teknologi informasi (TI). Standar ini dikembangkan untuk menggantikan sertifikasi British Standard (BS) 15000 yang ditetapkan oleh British Standards International (BSI). Dikembangkan sebagai proyek bersama oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC), standar ini juga dikenal sebagai IEC 20000. Tujuannya adalah untuk memungkinkan semua organisasi yang berpondasi pada teknologi informasi agar mampu menerapkan praktik terbaik.

Standar ini secara spesifik menentukan persyaratan bagi institusi (merujuk kepada BUMN, Swasta dan Government) penyedia layanan TI untuk merencanakan, menetapkan, menerapkan, mengoperasikan, memantau, mereview, memelihara dan meningkatkan sistem manajemen layanan TI.

Manfaat Sertifikasi ISO/20000

Sertifikasi ISO/IEC 20000 sangat penting bagi perusahaan karena mampu memberikan beberapa manfaat diantaranya adalah sebagai berikut:

1.Menunjukkan komitmen perusahaan dan meningkatkan daya saing.

Sertifikat ISO/IEC 20000 dapat meningkatkan citra perusahaan akan komitmennya terhadap kualitas layanan TI yang diberikan. Jika standar ISO 9000 menunjukkan komitmen perusahaan akan sistem manajemen mutu yang baik, maka ISO/IEC 20000 merupakan komitmen mutu yang baik dalam penyelenggaraan layanan TI. Pencapaian ini akan meningkatkan daya saing perusahaan di mata pelanggan.

2. Menunjukkan kemampuan perusahaan dalam audit.

Sertifikat ISO/IEC 20000 membuktikan bahwa penyedia layanan TI mampu memberikan layanan yang memenuhi kebutuhan pengguna. Di dalam standar ISO/IEC 20000 terdapat spesifikasi agar layanan yang diberikan memiliki kualitas yang dapat diterima oleh pelanggan. Sertifikat ISO 20000 mampu membuktikan kepada auditor bahwa layanan TI dikelola dengan baik dan kualitasnya dapat diterima oleh pelanggan. ISO 20000 menekankan pendekatan proses pada pengelolaan layanan TI, sehingga hal ini memberikan jaminan bahwa data yang dihasilkan oleh proses yang benar adalah data yang valid dan mereduksi keraguan auditor atas data yang diaudit.

3. Memenuhi persyaratan tender.

Standar ini wajib dimiliki oleh peyedia layanan eksternal yang ingin mengikuti tender. Beberapa tender mensyaratkan agar penyedia layanan telah tersertifikasi ISO/IEC 20000.

4. Memberikan kerangka kerja peningkatan layanan TI, mengurangi resiko dan biaya layanan TI.

Dengan mempraktekkan manajemen sistem layanan yang baik seperti yang ditetapkan dalam ISO/IEC 20000, diharapkan perusahaan dapat melakukan peningkatan dalam kualitas layanannya, melakukan penghematan biaya dan meningkatkan efisiensi, menghasilkan pengurangan resiko yang mungkin ditimbulkan oleh layanan TI dan mendorong perbaikan layanan TI secara terus-menerus.

Konsekuensi

Sertifikasi ISO 20000 membutuhkan usaha yang besar dari seluruh komponen manajemen layanan TI suatu institusi. Keberhasilannya ditentukan secara bersama-sama. Tiap-tiap orang/bagian memiliki porsi masing-masing untuk keberhasilan sertifikasi. Dibalik pencapaian tersebut, sudah pasti ada konsekuensi yang harus dipenuhi, antara lain:

-Jumlah biaya yang dikeluarkan untuk sertifikasi

Sertifikasi ISO 20000 tidak murah, perlu biaya yang relatif besar dikeluarkan. Namun, keberhasilnya akan mendatangkan keuntungan yang jauh lebih besar kepada institusi.

-Perlu usaha yang besar pada waktu pertama kali memutuskan melakukan sertifikasi

Usaha-usaha dimaksud adalah pelaksanaan manajemen layanan TI sebagaimana tercantum dalam ISO 20000, komitmen pimpinan untuk sungguh-sungguh menerapkan sistem manajemen layanan TI, merubah budaya kerja pegawai yang belum terbiasa dengan budaya kerja tercatat, terukur, terdokumentasi dan sesuai prosedur, penyesuain struktur organisasi manajemen layanan TI, pemenuhan teknologi (fasilitas, sarana dan prasarana kerja).

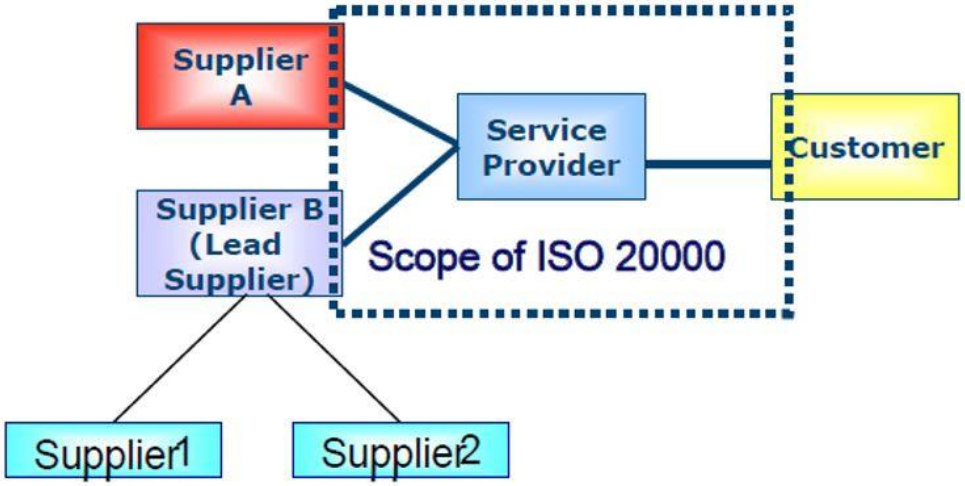
Jenis ISO 20000:

Secara formal ISO 20000 terdiri dari:

1. ISO 20000-1:2011, berisi tentang persyaratan sistem manajemen layanan TI yang harus dipenuhi oleh perusahaan agar layanan yang diberikan memiliki kualitas yang dapat diterima oleh pelanggan. Persyaratan yang dimaksud meliputi desain, transisi, pengiriman dan peningkatan layanan yang memenuhi persyaratan layanan dan memberikan nilai bagi pelanggan dan penyedia layanan. Persyaratan wajib dipenuhi perusahaan agar sesuai dengan standar. Bagian ini merupakan dasar bagi pihak ketiga dalam melakukan audit secara independen.
2. ISO 20000:2:2012, berisi petunjuk dalam penerapan sistem manajemen layanan TI. Bagian ini berisi saran untuk organisasi yang ingin melakukan sertifikasi.

3. ISO 20000:3-2009, berisi panduan tentang definisi ruang lingkup dan penerapan dari ISO 20000:1.
4. ISO 20000:4-2010, berisi proses model referensi.
5. ISO 20000-5:2010, berisi contoh implementasi rencana ISO 20000-1.

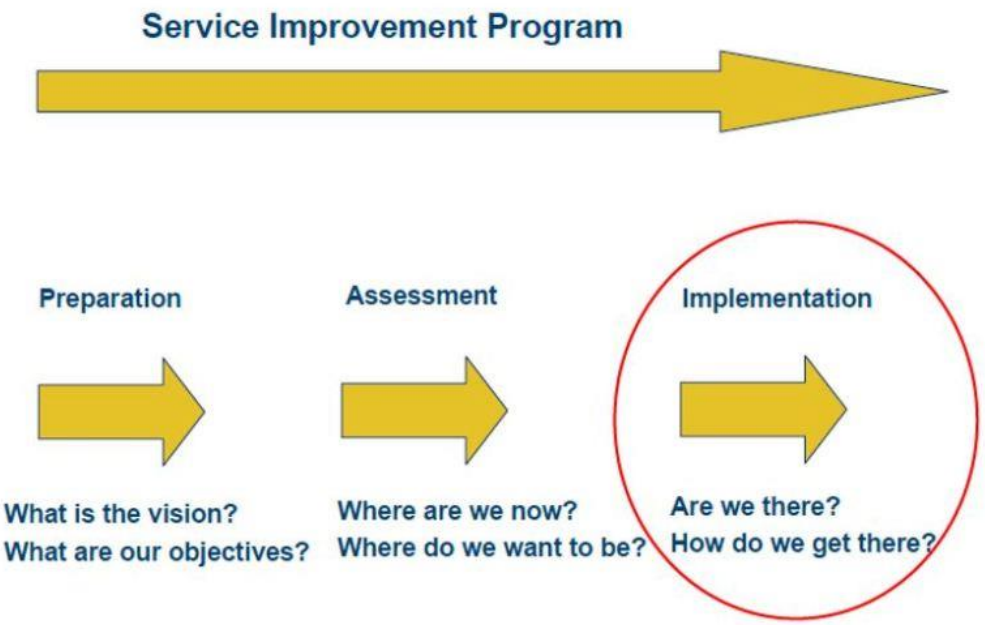
Standar ini menyediakan standar yang dapat digunakan untuk audit dan assessment penyedia layanan internal dalam organisasi atau industri dan pemasok eksternal dalam rantai pasok. Standar ini membantu organisasi menyediakan layanan yang berkualitas dan efektifitas dalam biaya lewat pengelolaan layanan yang profesional.



Gambar Area lingkup ISO/IEC 20000

Langkah-Langkah Mencapai Standarisasi ISO 20000:

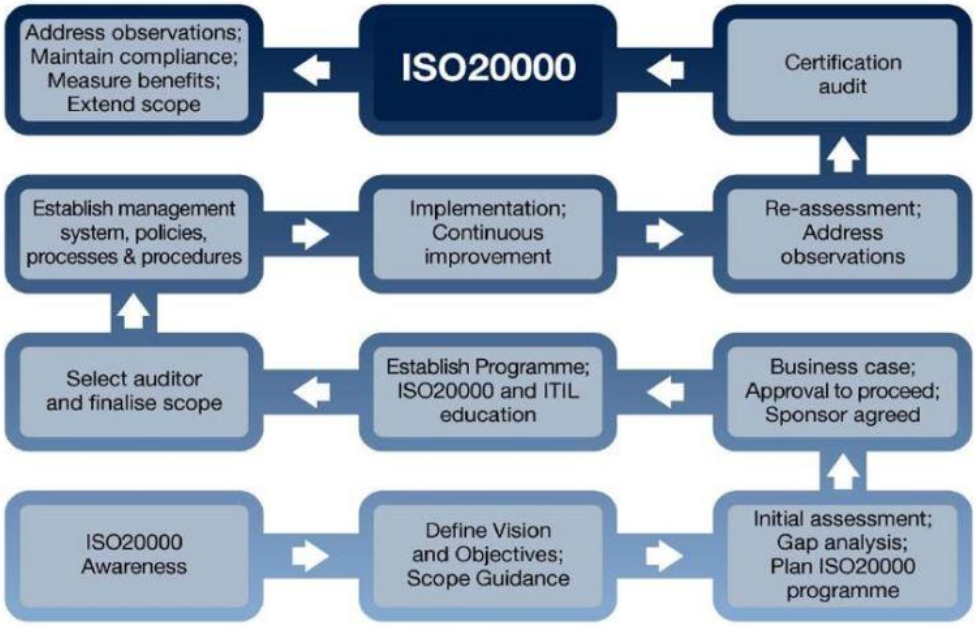
Standar ISO 20000 mengatur prosedur dan proses dari ITSM, sehingga diperlukan pemahaman dan implementasi ITSM. Perusahaan yang telah sadar akan pentingnya sertifikasi ISO 20000 untuk menjamin mutu layanan TI harus mendefinisikan visi dan misi yang dibantu dengan panduan batasan pengembangan kualitas. Kemudian dilakukan penilaian awal atas keadaan yang saat ini dialami perusahaan, dilanjutkan dengan gap analysis kondisi sekarang dengan kondisi yang ingin dicapai. Perusahaan selanjutnya perlu menyiapkan berbagai program perbaikan layanan berdasarkan temuan yang didapat dalam fase persiapan, penilaian, dan implementasi. Hal tersebut merupakan tahap awal mencapai ketentuan sertifikasi ISO 20000, yang tergambar pada bagan di bawah ini.



Gambar Bagan tahapan implementasi suatu program perbaikan layanan (John DiMaria, 2006)

Setelah perusahaan merencanakan manajemen layanan yang baik dan sesuai dengan best practice dan good practice yang ada, perusahaan mulai melakukan studi kasus agar persetujuan bisa diperoleh dan disetujui oleh sponsor. Langkah selanjutnya adalah menetapkan program yang berbasis pada ketentuan dan kriteria dalam ISO 20000 dan ITIL®. Diperlukan pemilihan auditor dan finalisasi lingkup layanan untuk kemudian dilanjutkan ke penetapan sistem manajemen, kebijakan-kebijakan, proses dan prosedur. Setelah proses dan prosedur ditetapkan, dimulailah implementasi manajemen layanan TI dan dilanjutkan dengan evaluasi dan perbaikan terus-menerus.

Setelah beberapa waktu menjalankan program manajemen layanan, dilakukan penilaian ulang dan pembahasan atas observasi yang dilakukan pihak auditor. Untuk dapat dikatakan certified, perusahaan perlu melakukan certification audit. Auditor atau tim audit akan memberikan serangkaian pertanyaan terkait dengan standar ISO 20000. Jika layanan dinyatakan telah layak dan mampu memberikan value bagi pelanggan, maka perusahaan akan mendapatkan sertifikat ISO 20000. Namun tidak berhenti sampai disini, perusahaan harus terus menerus melakukan observasi, mempertahankan kesesuaian layanan, mengukur manfaat dan memperluas lingkup manajemen layanan. Secara ringkas, langkah-langkah ini dapat dilihat dalam gambar.



Gambar Langkah-langkah mencapai sertifikat ISO 20000

ISO / IEC 27002: 2013

ISO / IEC 27002: 2013 memberikan pedoman untuk standar keamanan informasi organisasi dan praktik manajemen keamanan informasi termasuk pemilihan, penerapan, dan manajemen pengendalian dengan mempertimbangkan lingkungan risiko keamanan informasi organisasi.

Standar ini dirancang untuk digunakan oleh organisasi yang berniat untuk:

-pilih kontrol dalam proses penerapan Sistem Manajemen Keamanan Informasi berdasarkan ISO / IEC 27001;

-menerapkan kontrol keamanan informasi yang diterima secara umum;

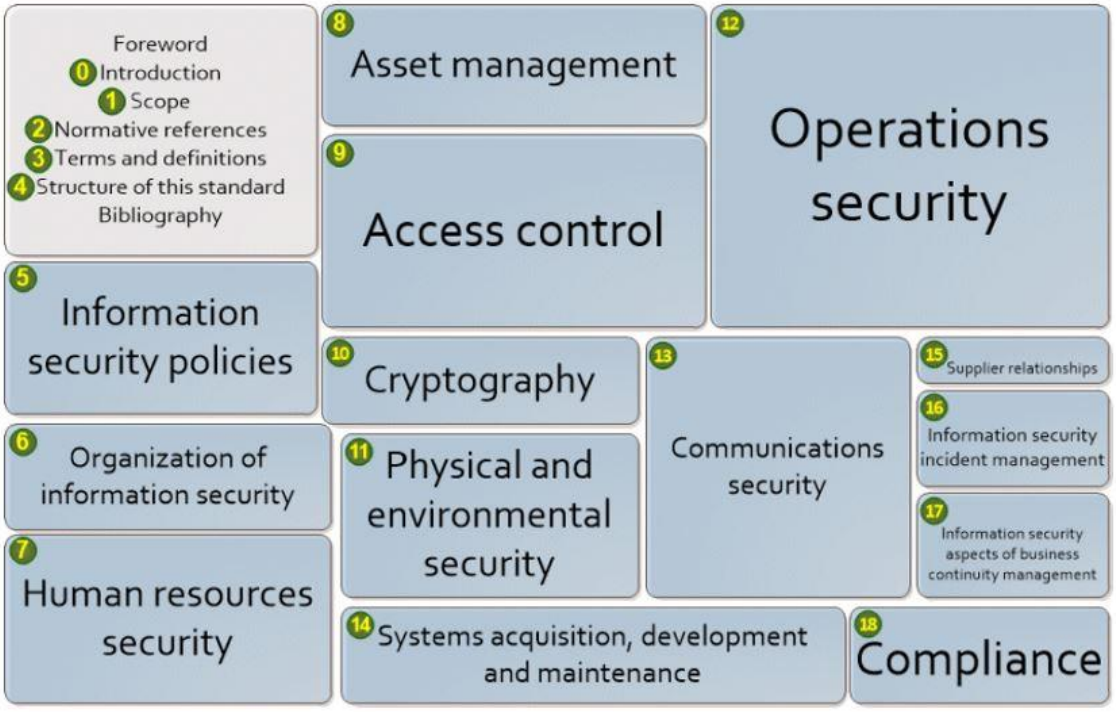
-mengembangkan panduan manajemen keamanan informasi mereka sendiri.

ISO/IEC 27002 merupakan standar praktik yang populer dan telah diakui secara internasional untuk keamanan informasi. Manajemen keamanan informasi adalah salah satu topik yang sangat vital dalam organisaai. Oleh karenanya ISO/IEC 27007 menjadi sangat relevan bagi berbagai macam organisasi yang menangani dan bergantung pada informasi termasuk perusahaan komersial dari yang kecil sampai yang perusahaan multinasional yang sangat besar, perusahaan non-profit, perusahaan amal, hingga pemerintahan.

Persyaratan risiko dan kontrol informasi mungkin berbeda bagi tiap-tiap organisasi, namun juga banyak persamaan seperti bagaimana setiap organisasi perlu membahas mengenai risiko informasi mengenai pegawai mereka dan kontraktor, konsultan dan supplier layanan informasi eksternal. Standarisasi ISO/IEC 27002 secara eksplisit berkaitan dengan keamanan informasi, yang berarti keamanan dalam berbagi betuk informasi seperti data komputer, dokumentasi, pengetahuan dan kekayaaan intelektual).

Struktur dan format ISO/IEC 27002:2013

ISO/IEC 27002:2013 merupakan kode praktik, dokumen umum yang bersifat penasihat, bukan spesifikasi formal seperti ISO / IEC 27001. Dokumen tersebut merekomendasikan kontrol keamanan informasi yang membahas tujuan pengendalian keamanan informasi yang timbul dari risiko terhadap kerahasiaan, integritas, dan ketersediaan informasi. Bagi organisai yang mengadopsi ISO/IEC 27002, harus menilai risiko informasi organisasinya, memperjelas tujuan kontrol dan menerapkan kontrol yang sesuai menggunakan standar sebagai panduan.



Gambar Bagian-Bagian Kontrol pada ISO 27002

Standarisasi dimulai dengan 5 bab pengantar:

1. Introduction
2. Scope
3. Normative references
4. Terms and definitions
5. Structure of this standar

Dan diikuti oleh 14 bab utama:

- Kebijakan Keamanan Informasi
- Organisasi Keamanan Informasi
- Keamanan Sumber Daya Manusia
- Manajemen aset
- Kontrol akses
- Kriptografi
- Keamanan fisik dan lingkungan
- Operasi Keamanan- prosedur dan tanggung jawab, Perlindungan dari malware, Pencadangan, Penebangan dan pemantauan, Pengendalian perangkat lunak operasional, Pengelolaan kerentanan teknis dan koordinasi koordinasi sistem informasi
- Keamanan komunikasi – Manajemen keamanan jaringan dan transfer Informasi
- Akuisisi sistem, pengembangan, dan pemeliharaan – Persyaratan keamanan sistem informasi, Keamanan dalam proses pengembangan dan dukungan, serta data Uji
- Hubungan pemasok – Keamanan informasi dalam hubungan pemasok dan manajemen pengiriman layanan Pemasok
- Manajemen insiden keamanan informasi – Manajemen insiden keamanan informasi dan perbaikan
- Aspek keamanan informasi manajemen kontinuitas bisnis – kontinuitas keamanan informasi dan Redudansi
- Kepatuhan – Kepatuhan dengan persyaratan hukum dan kontrak dan tinjauan keamanan Informasi

BAGIAN UTAMA DARI STANDAR:

Bagian utama dari standar diatur di bagian-bagian berikut, yang sesuai dengan kontrol keamanan informasi. Perlu diingat bahwa organisasi dapat menggunakan pedoman ini sebagai dasar untuk pengembangan ISMS. Sebagai berikut:

Bagian 5 – Kebijakan Keamanan Informasi

Dokumen harus dibuat pada kebijakan keamanan informasi perusahaan, yang berisi konsep keamanan informasi, struktur untuk menetapkan tujuan dan bentuk kontrol, komitmen manajemen terhadap kebijakan, di antara banyak faktor lainnya.

Bagian 6 – Pengorganisasian Keamanan Informasi

Untuk menerapkan Keamanan Informasi dalam suatu perusahaan, perlu dibentuk kerangka kerja untuk mengelolanya dengan baik. Untuk ini, kegiatan keamanan informasi harus dikoordinasikan oleh perwakilan dari organisasi, yang harus memiliki tanggung jawab yang jelas, melindungi informasi yang bersifat rahasia.

Bagian 7 – Manajemen Aset

Aset, menurut norma, adalah segala sesuatu yang bernilai bagi organisasi dan yang perlu dilindungi. Untuk ini, aset harus diidentifikasi dan dikelompokkan sehingga inventaris dapat disusun dan dipelihara. Selain itu, mereka harus mengikuti aturan yang terdokumentasi, yang menentukan jenis penggunaan apa yang diizinkan untuk aset tersebut.

Bagian 8 – Keamanan Sumber Daya Manusia

Sebelum mempekerjakan karyawan – atau bahkan pemasok -, penting bahwa mereka dianalisis dengan benar, terutama jika mereka berurusan dengan informasi sensitif. Maksud dari bagian ini adalah untuk mengurangi risiko pencurian, penipuan atau penyalahgunaan sumber daya. Ketika beberapa karyawan bekerja di perusahaan, mereka harus sadar akan ancaman keamanan informasi, serta tanggung jawab dan kewajiban mereka.

Bagian 9 – Keamanan fisik dan lingkungan

Peralatan dan fasilitas untuk pemrosesan informasi kritis atau sensitif harus dipelihara di area yang aman, dengan level yang sesuai dan kontrol akses, termasuk perlindungan terhadap ancaman fisik dan lingkungan.

Bagian 10 – Operasi dan Komunikasi Keamanan

Penting untuk mendefinisikan prosedur dan tanggung jawab untuk manajemen dan operasi semua sumber daya pemrosesan informasi. Ini termasuk manajemen layanan yang dialihkan, perencanaan sumber daya sistem untuk meminimalkan risiko kegagalan, pembuatan cadangan dan prosedur pemulihan, dan administrasi jaringan komunikasi yang aman.

Bagian 11 – Kontrol Akses

Akses ke informasi, serta sumber daya pemrosesan informasi dan proses bisnis, harus dikontrol berdasarkan persyaratan bisnis dan keamanan informasi. Akses pengguna yang sah serta mencegah akses tidak sah ke sistem informasi harus dipastikan, untuk menghindari kerusakan pada dokumen dan sumber pemrosesan informasi yang tersedia bagi siapa saja.

Bagian 12 – Akuisisi, pengembangan dan pemeliharaan sistem

Persyaratan keamanan sistem informasi harus diidentifikasi dan disepakati sebelum pengembangan dan / atau implementasi, sehingga mereka dapat dilindungi untuk menjaga kerahasiaan, keaslian atau integritas mereka dengan cara kriptografi.

Bagian 13 – Manajemen Insiden Keamanan Informasi

Pendaftaran formal dan prosedur eskalasi harus ditetapkan; karyawan, pemasok, dan pihak ketiga harus mengetahui prosedur pelaporan kejadian keamanan informasi untuk memastikan bahwa laporan tersebut dilaporkan secepat mungkin dan dikoreksi secara tepat waktu.

Bagian 14 – Manajemen Kelangsungan Bisnis

Rencana kesinambungan bisnis harus dikembangkan dan diimplementasikan untuk mencegah gangguan aktivitas bisnis serta untuk memastikan bahwa operasi inti dengan cepat pulih.

Bagian 15 – Kepatuhan

Penting untuk menghindari pelanggaran hukum pidana atau perdata, memastikan undang-undang, peraturan atau kewajiban kontraktual serta persyaratan keamanan informasi. Jika perlu, perusahaan dapat menyewa konsultan khusus untuk memverifikasi kepatuhan dan kepatuhannya terhadap persyaratan hukum dan peraturan.

KEUNTUNGAN:

Keuntungan yang diberikan oleh sertifikasi ISO adalah perwakilan untuk perusahaan, terutama karena telah diakui di seluruh dunia.

Kesadaran keamanan informasi yang lebih baik;

Kontrol yang lebih besar atas aset dan informasi sensitif;

Menyediakan pendekatan untuk implementasi kebijakan kontrol;

Kesempatan untuk mengidentifikasi dan memperbaiki kelemahan;

Mengurangi risiko tanggung jawab karena tidak menerapkan ISMS atau menentukan kebijakan dan prosedur;

Ini menjadi perbedaan kompetitif untuk pencapaian pelanggan yang menghargai sertifikasi;

Organisasi yang lebih baik dengan proses dan mekanisme yang dirancang dan dikelola dengan baik;

Mendorong pengurangan biaya dengan pencegahan insiden keamanan informasi;

Kepatuhan dengan undang-undang dan peraturan lainnya.