**Sertifikasi ISO 27001 | Sertifikat ISO 14001 | Sertifikat ISO 27001**

Semua sistem manajemen berdasarkan standar ISO memiliki satu kesamaan: siklus Deming atau PDCA (Plan, Do, Check, dan Act) yang diketahui, yang dapat mempermudah integrasi berbagai standar ISO dalam organisasi: ISO 9001, ISO 14001, ISO 27001, ISO 20000, dll. Saya tahu perusahaan yang memiliki ISO 27001, tetapi mereka harus lebih fokus pada manajemen layanan TI, sehingga mereka menerapkan ISO 20000. Dan sebaliknya - Saya tahu perusahaan yang memiliki ISO 20000, tetapi mereka perlu lebih fokus pada keamanan informasi dan menerapkan ISO 27001.

Dalam kasus ISO 27001 dan ISO 20000, integrasi ini dapat melampaui PDCA, seperti yang akan kita lihat di bawah ini - ada kontrol keamanan dalam Lampiran A dari ISO 27001 yang dapat dikelola sebagai proses dalam ISO 20000.

**Elemen manajemen serupa di ISO 27001 dan ISO 20000**

Mari kita ingat poin ISO 27001 / ISO 20000 mana, yang terkait dengan PDCA, yang dapat diintegrasikan pada saat menerapkan **Sertifikasi ISO 27001** dan Sertifikasi ISO 20000 (sistem yang dihasilkan mengintegrasikan kedua standar, dan disebut sebagai "sistem terintegrasi" atau "manajemen terpadu" sistem"):

- **Kebijakan:** Menetapkan aturan internal untuk pengelolaan sistem terintegrasi.
- **Definisi tujuan:** Menentukan tujuan yang ingin dicapai dengan implementasi sistem terintegrasi. Ini juga akan melibatkan definisi beberapa indikator untuk mengukur apakah tujuan telah tercapai.
- **Definisi peran dan tanggung jawab:** Menentukan peran dan tanggung jawab untuk pengelolaan sistem terintegrasi. Biasanya mendefinisikan orang yang bertanggung jawab untuk sistem terintegrasi. Juga menetapkan Komite yang terintegrasi dengan manajemen senior sebagai peserta utama.
- **Kesadaran:** Semua personil yang dipengaruhi oleh ruang lingkup sistem manajemen terpadu harus dididik dengan baik dalam keamanan informasi dan manajemen layanan.

- **Komunikasi:** Komunikasi internal dan eksternal yang terkait dengan sistem manajemen terpadu harus dilakukan dengan menetapkan pedoman (biasanya didefinisikan sebagai protokol komunikasi).
- **Pengendalian dokumen dan catatan:** Anda harus menetapkan pedoman untuk pengelolaan semua dokumentasi dan catatan dari sistem terintegrasi.
- **Manajemen metrik:** Dalam kasus Sertifikat ISO 27001, Anda harus menetapkan metrik untuk mengukur efektivitas kontrol keamanan, sedangkan dalam kasus Sertifikat ISO 20000 Anda harus menetapkan metrik untuk mengukur efektivitas proses.
- **Audit internal:** Anda harus melakukan realisasi audit internal untuk mendeteksi kemungkinan ketidaksesuaian dalam sistem terintegrasi, dan menentukan tingkat implementasi terkait standar referensi.
- **Tinjauan manajemen:** Manajemen puncak organisasi harus meninjau serangkaian titik masuk untuk sistem manajemen terpadu. Sebagai hasil dari tinjauan, mereka harus menghasilkan beberapa kesimpulan atau hasil.
- **Tindakan korektif / preventif dan peningkatan berkelanjutan:** Manajemen sistem terintegrasi dapat mengembangkan tindakan korektif dan preventif untuk pengobatan ketidaksesuaian yang terdeteksi (biasanya terdeteksi dalam audit, tinjauan, dll.). Dalam kasus ISO 27001, tidak ada referensi untuk tindakan pencegahan, yang mungkin sama di versi ISO 20000 berikutnya. (Sesuatu yang serupa terjadi dengan sisa standar ISO, mengingat perubahan yang terjadi pada tingkat umum untuk integrasi yang lebih besar antara semua standar ISO.)