Uma abordagem integrada para sistemas de gestão

Incluindo um elemento de segurança da informação

Mudando para padronização

As demandas atuais do mercado exigem que as empresas considerem uma ampla variedade de componentes que definem o sucesso. Sistemas e processos de gestão implementados de forma eficaz podem apoiar todos os fatores da eficácia organizacional. Eles também ajudam a introduzir uma mentalidade de melhoria contínua que está no âmago de toda empresa eficiente.

A ISO 9001 é a norma internacional que define os requisitos de um sistema de gestão da qualidade. Desde que ela foi introduzida, mais de um milhão de organizações obtiveram a certificação. É agora uma das obras mais significativas já escritas na literatura de negócios.

Após o sucesso da ISO 9001, muitas normas adicionais foram publicadas e mais organizações começaram a implementar vários sistemas de gestão, cada um exigindo certificações separadas realizadas por uma terceira parte. Como resultado, ficou claro que a falta de consistência na estrutura e no conteúdo das diferentes normas ISO dificultava muito uma abordagem mais integrada. Como solução, a ISO introduziu o Anexo SL.

LRQA

O papel do Anexo SL

O Anexo SL é a estrutura que todas as normas novas e revisadas de sistemas de gestão ISO seguem.

Para garantir que as normas sejam consistentes e compatíveis entre si, o Anexo SL inclui quatro temas principais:

Estrutura de alto nível

Essa é a base do Anexo SL e apresenta dez cláusulas, que vão do escopo ao planejamento e melhoria.

Ela reduz drasticamente a duplicação de esforços porque os sistemas de gestão seguem o mesmo conjunto de requisitos básicos.

Texto central idêntico

No mínimo, as normas de sistema de gestão terão 84 requisitos genéricos, além de quaisquer requisitos adicionais específicos da área.

Isso ajuda a garantir que os materiais relacionados às normas sejam claros, repetíveis e facilmente assimilados por aqueles que trabalham em várias áreas.

Termos e definições comuns

Há 22 termos e definições que devem ser explicados em todas as normas. Por exemplo, “parte interessada” é o termo preferível a “stakeholder” e “liderança” substitui “responsabilidade da direção”.

Abordagem baseada em risco

O Anexo SL ajuda as organizações a adotar uma abordagem sistemática e proativa em relação ao risco. Isso minimiza a ocorrência e o impacto de eventos indesejados e promove a melhoria contínua.

Cláusula 1	Escopo
Cláusula 2	Referências normativas
Cláusula 3	Termos e definições
Cláusula 4	Contexto da organização
Cláusula 5	Liderança
Cláusula 6	Planejamento
Cláusula 7	Suporte
Cláusula 8	Operação
Cláusula 9	Avaliação de desempenho
Cláusula 10	Melhoria

Estrutura de alto nível do Anexo SL

Facilidade de implementação

A compatibilidade que o Anexo SL apresenta facilita a integração dos requisitos de várias normas em um único sistema. Em resultado disso, agora é muito mais simples para uma organização adicionar novos sistemas de gestão baseados no Anexo SL e combiná-los com os existentes.

Essa é uma abordagem mais prática que minimiza a duplicação e cria um sistema em que muitas partes impulsionam o mesmo conjunto de objetivos estratégicos. O Anexo SL também fornece às organizações uma estrutura de melhores práticas para gerenciar outros processos que não foram escolhidos para certificação.

Por meio da integração, as organizações podem usar seus recursos com mais eficiência e adotar uma abordagem padronizada para a documentação. Também podem melhorar sua gestão de operações e processos cruciais.

Estudo de caso

Terex Trucks

A Terex Trucks foi uma das primeiras organizações a fazer a transição para a ISO 9001:2015.

Graças ao Anexo SL, a Terex Trucks se beneficiou dos pontos em comum entre as normas. Isso permitiu a integração dos sistemas de qualidade (SGQ) e gestão ambiental (SGA) da organização.

“Há muitos pontos em comum entre as duas normas [ISO 9001 e ISO 14001] e, como agora ambas seguem a estrutura introduzida pelo Anexo SL, pudemos aprender com o trabalho que realizamos em nosso SGQ para integrar nosso SGA ao mesmo tempo.

Nossas estatísticas de desempenho confirmam que cumprimos com sucesso nossos objetivos para o SGQ e o SGA, e continuaremos a ampliar isso no futuro por meio da implantação do nosso sistema de gestão.”

Processo de certificação otimizado

As vantagens da integração não se limitam à implementação de sistemas de gestão.

Quando uma organização nomeia um organismo de certificação, como o LRQA, as auditorias integradas conduzem a uma abordagem mais eficiente. Por exemplo, talvez a estrutura de alto nível precise ser revisada apenas uma vez, o que pode reduzir o número de visitas necessárias ao local.

Por meio da integração, as organizações também constroem relacionamentos de longo prazo com os organismos de certificação e os auditores.

Com a exposição a vários sistemas, os auditores desenvolvem um conhecimento íntimo e holístico da empresa, de seus objetivos e do seu método de operação. Isso permite entregar perspectivas mais profundas que têm um impacto maior.

Avaliação remota

Ao trabalhar com o LRQA, as organizações podem, em muitos casos, optar por fazer suas auditorias remotamente, usando tecnologia segura e protegida. Essa opção oferece o mesmob serviço de alta qualidade com vários benefícios adicionais, incluindo flexibilidade, entrega rápida e acesso a conhecimento global.

As empresas também podem optar por uma abordagem mista que otimiza o processo geral usando auditorias remotas e, ao mesmo tempo, utilizando opções presenciais para ajudar a construir relacionamentos pessoais sólidos.

Todos os clientes do LRQA que escolhem uma auditoria remota se beneficiam da flexibilidade e conveniência que ela oferece.

Mas ela também mostra às organizações como a tecnologia estabelecida pode ser aproveitada para realizar uma auditoria eficaz que não é limitada por fronteiras geográficas. Isso ajuda algumas empresas a identificar como podem usar tecnologia e plataformas semelhantes para seus próprios programas internos de supervisão e auditoria.

Incluindo a ISO 27001 no seu sistema de gestão integrado

A ISO 27001 é a norma internacional que descreve os requisitos de um sistema de gestão de segurança da informação (SGSI).

Para qualquer organização, independentemente do tamanho ou do setor, a ISO 27001 fornece uma base sólida para uma estratégia abrangente de segurança cibernética e da informação. Ela descreve uma estrutura de melhores práticas para mitigar riscos e proteger informações críticas de negócios por meio de identificação, análise e controles acionáveis.

Incluir a ISO 27001 em um sistema de gestão integrado mais amplo é a maneira ideal de garantir que, como área de foco estratégico, as melhores práticas de segurança da informação sejam incorporadas à organização.

Integração da ISO 27001 com a ISO 9001

Graças ao Anexo SL, está se tornando cada vez mais popular integrar a

ISO 27001 e a ISO 9001. As duas normas compartilham uma estrutura semelhante e enfocam questões internas e externas, embora de ângulos específicos em áreas diferentes.

A integração dos requisitos de ambas as normas em um único sistema garante que os processos da organização estejam alinhados.

As semelhanças entre as normas também oferecem a oportunidade de acelerar a implementação e usar os recursos de forma mais eficiente.

Para cada norma, os requisitos específicos são diferentes. Contudo, como exemplo, as seguintes áreas comuns podem ser abordadas usando os mesmos processos e sistemas, levando a resultados diferentes:

- Partes interessadas
- Responsabilidades
- Documentação do sistema de gestão
- Auditoria interna e análise da direção
- Sistemas para não conformidades e ações corretivas

Ampliação do seu sistema para gerenciar riscos específicos à segurança da informação

Dependendo do perfil de risco de uma organização, outras normas e diretrizes permitem uma oportunidade de expandir o sistema para lidar com ameaças mais específicas.

A ISO 27001 faz parte da série de normas ISO 27000. Na família ISO 27000, existem várias outras normas e diretrizes, que são extensões da ISO 27001.

Essas normas e diretrizes adicionais descrevem os controles relacionados a áreas como privacidade e proteção de dados (ISO 27701, ISO 27018) e segurança na nuvem (ISO 27017). O cumprimento de normas adicionais como essas fortalece ainda mais o elemento de segurança da informação de um sistema integrado e assegura que esteja em operação uma abordagem mais robusta e abrangente para a gestão de riscos.

Também é comum as organizações expandirem seu sistema integrado para abranger a continuidade dos negócios (ISO 22301) e, quando relevante, a gestão de serviços de TI (ISO 20000-1).

Estudo de caso

OCTO Telematics

Uma abordagem de sistemas de gestão integrados

A OCTO Telematics (OCTO) é uma fornecedora líder em serviços telemáticos e análise avançada de dados para o setor de seguros.

A OCTO implementou um sistema de gestão abrangente e integrado que foi auditado e certificado pelo LRQA.

Ele ajuda a organização a acompanhar o cenário de ameaças à segurança da informação em constante evolução, reduzindo os riscos de forma proativa antes que eles ocorram.

"A estrutura de alto nível do Anexo SL, com seu texto básico idêntico, termos e definições comuns, facilitou a integração de nossos sistemas de gestão."

"Por meio da integração, a OCTO conseguiu minimizar o conflito entre sistemas individuais. Também reduziu a duplicação de processos, o trabalho administrativo e a burocracia geral. Isso garantiu um foco muito mais forte nas necessidades do negócio como um todo, em vez de em uma área em particular."

"Um SGSI certificado é a porta para garantir negócios com clientes importantes. No entanto, também permitiu que a OCTO adotasse uma abordagem orgânica à segurança do sistema — por meio da extensão do SGSI para gerenciar adequadamente as ameaças e oportunidades relacionadas ao nosso negócio."

Attilio De Bernardo | Diretor de Segurança da Informação OCTO Telematics

Criando seu sistema de gestão integrado com o LRQA

Entendemos que sua organização tem requisitos exclusivos. Independentemente de ser uma empresa de pequeno ou médio porte que procura dar os primeiros passos em direção a um sistema de gestão integrado ou uma grande empresa que busca níveis adicionais de segurança, nossa equipe de especialistas trabalhará de perto com você para entender suas necessidades específicas.

O LRQA oferece uma variedade de serviços de auditoria acreditada, certificação e treinamento relacionados às normas e esquemas líderes mundiais, para áreas que variam da segurança da informação até qualidade ou saúde e segurança.

Saiba mais

Fale com a nossa equipe para a construção de uma solução baseada nos requisitos da sua organização. Envie um e-mail para **brasil@lrqa.com** para marcar uma consulta.

YOUR FUTURE. OUR FOCUS.

Sobre LRQA:

Ao reunir experiência incomparável em inspeção, certificação, garantia de marca, segurança cibernética e treinamento, nos tornamos um provedor líder global de garantia.

Estamos orgulhosos de nossa herança, mas é quem somos hoje que realmente importa, porque é isso que molda a forma como faremos parceria com nossos clientes amanhã. Combinando fortes valores, décadas de experiência em gestão e mitigação de riscos e um grande foco no futuro, estamos aqui para apoiar nossos clientes enquanto eles constroem negócios mais seguros, mais seguros e mais sustentáveis.

De inspeção independente, certificação e auditoria; aos serviços de treinamento e assessoria técnica; à tecnologia de garantia em tempo real; para a transformação da cadeia de suprimentos baseada em dados, nossas soluções inovadoras de ponta a ponta ajudam nossos clientes a gerenciar um cenário de risco em rápida mudança - certificando-se de que eles estão moldando seu próprio futuro, em vez de permitir que ele os molde.

Entre em contato

LRQA Brasil
www.lrqa.com/br
+55 11 3523 3940