マネジメントシステムへの統合アプローチ

情報セキュリティの要素の追加

標準化への移行

今日の市場では、企業は成功を定義する多種多様な要素を検討する必要があります。効果的に導入されているマネジメントシステムとプロセスは、組織の有効性を生むすべての原動力の支えとなります。また、優秀なビジネスの核となる継続的改善の考え方の導入にも役立ちます。

品質マネジメントシステムの要求事項を規定する国際規格である ISO 9001 が導入されて以来、100 万以上の組織が認証を取得しています。IOS 9001 は今までに作成されたビジネス文献の中でも最も重要な規格の一つです。

ISO 9001 の成功に続いて、多くの規格が発行され、より多くの組織が、第三者による認証を必要とする複数のマネジメントシステムの導入を開始しました。その結果、異なる ISO 規格の構造と内容の一貫性が欠如しており、より統合的なアプローチをとることが非常に困難になっていることが明らかになり、解決策として、ISO が導入したのが Annex SL です。

Annex SL（附属書 SL）の役割

Annex SL は、すべての新規および改訂された ISO マネジメントシステム規格が参考とする枠組みです。

規格の整合性と互換性を確実にするため、Annex SL には 4 つの主要テーマがあります。

上位構造

これは Annex SL の基盤であり、適用範囲から計画、改善まで 10 の条項があります。マネジメントシステムが一連の同じ基本要求事項に従うことで、作業の重複を大幅に削減します。

共通の中核となるテキスト

マネジメントシステムの規格は、少なくとも 84 の一般要件があり、それに加え、分野固有の他の要件があります。

これにより、規格に関連する資料が明確かつ再現性を有し、複数の領域で作業する人の容易な理解を確実に促します。

共通の用語および定義

すべての規格で扱う必要がある用語と定義は 22 項目あります。例えば、「利害関係者（interested party）」は「ステークホルダー（stakeholder）」より好まれる用語であり、「経営者の責任（management responsibility）」 は「リーダーシップ（leadership）」に置き換えられます。

リスクベースのアプローチ

Annex SL は、組織がリスクに対して体系的かつ積極的なアプローチを採用することを支援します。これにより、望ましくない事象の発生と影響を最小限に抑え、継続的改善を促します。

条項 1	適用範囲
条項 2	引用規格
条項 3	用語および定義
条項 4	組織の状況
条項 5	リーダーシップ
条項 6	計画
条項 7	支援
条項 8	運用
条項 9	パフォーマンス評価
条項 10	改善

導入の容易さ

Annex SL が提供する互換性により、複数の規格の要件事項を単一のシステムに容易に統合することができます。その結果、組織が Annex SL に基づく新たなマネジメントシステムを追加し、既存のシステムと統合することが非常に容易になりました。

これは、重複を最小限に抑え、多くの要素が同じ戦略目標に向かうシステムを作る、より実用的なアプローチです。また、Annex SL は、認証対象として選択されなかったその他のプロセスを管理するためのベストプラクティス・フレームワークも組織に提供します。

統合を通じて、組織はより効率的にリソースを使用し、より規格化された文書化のアプローチをとることができ、重要なオペレーションおよびプロセスの運用管理も向上させることができます。

ケーススタディ

テレックストラック

テレックストラックは ISO 9001：2015 に初期に移行した組織の一つです。

Annex SL のおかげで、テレックストラックは規格間で共通する点による恩恵を受け、組織の品質（QMS）と環境マネジメントシステム（EMS）の統合が可能になりました。

“ISO 9001 と ISO 14001 の 2 つの規格には多くの共通点があり、どちらも Annex SL で導入された構造に従っているため、QMS で完了した作業から学び、それと同時に EMS を統合することが可能になりました。

パフォーマンス統計からは、当社が QMS と EMS の目標を成功裏に達成したことが確認できており、今後も、当社のマネジメントシステムの展開を通じて発展させていきたいと思います。”

最適化された認証プロセス

統合の利点は、マネジメントシステムの導入に限定されません。

組織が LRQA のような認証機関を任命する場合、統合審査によるさらに効率的なアプローチが促されます。例えば、上位構造の評価の必要性は一度のみにすることができ、必要とされるサイト訪問の回数を減らすことができます。

また、統合を通じて、組織は認証機関や審査員との長期的な関係を構築します。

複数のシステムに関わることでで、審査員はビジネスおよびその目標、ならびにその手法に関する詳細で全体的な知識を身に付けるため、より大きな影響をもたらし、より深い洞察を提供することが可能になります。

デジタルアシュアランス（デジタル上での審査）

LRQA のサービスをご利用いただく組織は、多くの場合、安全で信頼できるテクノロジーを用いたリモート方式での審査を選ぶことができます。リモートにおいても、柔軟性や迅速な提供、グローバルな専門知識へのアクセスなど、いくつものメリットが加わった、オンサイトと同じ高品質のサービスを受けることができます。

また企業は、リモート審査を行う一方で、オンサイトでの審査オプションを活用して、強力な人間関係の構築を促し、全体のプロセスを最適化するハイブリッド型のアプローチを選ぶこともできます。

リモート審査を選択する全てのお客様は、リモート審査から提供される柔軟性と利便性というメリットを享受すると確信しています。さらに、地理的な境界に制限されない効果的な審査を実行するために、主流のテクノロジーを活用する方法も組織に提示し、企業が、社内の監視や審査プログラムのテクノロジーおよびプラットフォームを使用する方法を特定するのにも役立ちます。

統合マネジメントシステムへの ISO 27001 の包含

情報セキュリティ・マネジメントシステム（ISMS）の要求事項を定義する国際規格、それが ISO 27001 です。

規模やセクターに関係なく、どのような組織にとっても、ISO 27001 は包括的な情報およびサイバーセキュリティ戦略の強固な基盤を提供します。また、リスクを軽減し、識別、分析、実行可能な管理を通じて、ビジネスにとって重要な情報を保護するためのベストプラクティス・フレームワークの概要を示します。

ISO 27001 をより広範な統合マネジメントシステムに含めることは、戦略的重点分野として、情報セキュリティのベストプラクティスを組織内に確実に組み込むための理想的な方法です。

ISO 27001 と ISO 9001 の統合

Annex SL のおかげで、ISO 27001 と ISO 9001 の統合は一般的になっています。それぞれ異なる専門分野固有の視点からですが、どちらの規格も似たような構造を共有しており、内部と外部の問題に焦点を当てています。

両方の規格の要件事項を単一のシステムに統合することで、組織のプロセスの整合性が確保されます。また、規格間の類似性は、導入スピードを速め、リソースをより効率的に使用する機会を提供します。

各規格では、特定の要件事項が異なります。しかし、例として、以下の共通領域は、同じプロセスおよびシステムを使用して対処することができますが、異なる結果をもたらします。

- 利害関係者
- 職責
- 文書マネジメントシステム
- 内部監査・マネジメントレビュー
- 不適合と是正処置のためのシステム

特定の情報セキュリティ・リスクを管理するためのシステムの拡張

組織のリスクプロファイルに応じて、より具体的な脅威に対応するために、他の規格やガイドラインによってシステムを拡張する機会を得られます。

ISO 27001 は、ISO 27000 シリーズの規格の一部です。ISO 27000 ファミリーの中には、ISO 27001 を拡張した、いくつかの他の規格やガイドラインが存在します。

これらの追加の規格およびガイドラインは、プライバシーおよびデータ保護（ISO 27701、ISO 27018）やクラウドセキュリティ（ISO 27017）などの分野に関連する統制の概要を示しています。このような追加の規格に準拠することで、統合システムの情報セキュリティ・エレメントがさらに強化され、運用のリスクマネジメントに対するより強固で広範なアプローチを確実にします。

また、組織が統合システムを拡張し、事業継続（ISO 22301）や、必要に応じて IT サービスマネジメント（ISO 20000-1）を対象に含めることも一般的です。

ケーススタディ

OCTO テレマティクス

OCTO テレマティクス（OCTO）は、保険産業のテレマティクス・サービスおよび高度なデータ分析の大手プロバイダです。

OCTO は、LRQA が認証および審査した包括的な統合マネジメントシステムを導入しました。絶えず進化する情報セキュリティ脅威の状況に、組織が継続して対応し、リスクが発生する前に積極的にリスクを軽減します。

“Annex SL の上位構造は、共通の中核となるテキスト、共通の用語および定義を有するため、マネジメントシステムの統合が容易になりました。”

“OCTO は、今回の統合により、個別のシステム間の対立を最小限に抑えることができました。また、プロセス、事務作業、全体的に煩雑な手続きの重複も減少し、特定の単一の領域ではなく、ビジネス全体のニーズにさらに強いフォーカスが向けられるようになりました。”

“認定された ISMS は、重要な顧客とのビジネスを確保するための入り口ですが、それはまた、OCTO がシステム・セキュリティに対する系統的なアプローチをとることを可能にしました。つまり、ISMS の拡張による、ビジネスに関連する脅威と機会の適切な管理です。”

アッティリオ・デ・ベルナルド
最高情報セキュリティ責任者
OCTO テレマティクス

LRQA で統合マネジメントシステムを構築

LRQA は、お客様の組織には独自の要求事項があることを理解しています。統合マネジメントシステムに向けた最初のステップをとろうと考えている中小企業でも、追加レベルの保証を検討している大企業でも、当社の専門家チームは、お客様と寄り添って独自のニーズの把握に努めます。

LRQA は、情報セキュリティから品質、安全衛生に至るまで、世界をリードする規格およびスキームに関する幅広い認定審査、認証および教育・トレーニングサービスを提供しています。

お問い合わせ

詳細については
https://www.lrqa.com/ja-jp/
をご覧ください。

YOUR FUTURE. OUR FOCUS.

LRQA について：

認証、ブランド認証、食品安全、サイバーセキュリティ、インスペクション、教育研修分野の比類なき専門知識を結集することにより、当社は世界的な認証のリーディングプロバイダーの地位を確保しています。

その伝統は誇るべきものですが、顧客との今後のパートナー関係を構築する上で、本当に重要なのは現在の当社の姿です。揺るぎない価値、リスク管理・軽減における数十年の経験、未来への的確なフォーカスを組み合わせることで、より安心・安全・持続可能なビジネス構築に向けてお客様をいつでも支援します。

独立した審査・認証・教育研修から、技術アドバイザリーサービス、リアルタイムの認証技術、データによるサプライチェーン改革まで、当社の革新的なエンドツーエンドのソリューションが、変化の速いリスク環境に積極的に対処できるようお客様をサポートします。つまり、未来の状況を成り行きに任せるのではなく、お客様が自ら構築できるようになるのです。

お問い合わせ

詳細については
https://www.lrqa.com/ja-jp/
をご覧ください。

LRQA リミテッド
〒 220-6010
横浜市西区みなとみらい 2-3-1
クイーンズタワー A10 階

本書に示すすべての情報が正確かつ最新であるように、LRQA リミテッドでは細心の注意を払っています。ただし、情報の不正確さや変更について当社は一切の責任を負いません。

LRQA は、LRQA Group Limited およびその子会社の商号です。詳細については www.lrqa.com/entities をご参照ください。

© LRQA Group Limited 2021