NKKKQA

ISO27001情報セキュリティマネジメントシステム審査認証

情報セキュリティマネジメントシステムとは

情報セキュリティマネジメントシステム(ISMS)とは組織が重要と考える「情報」に関して、機密を守り(機密性)、誤使用や改竄を防ぎ(完全性)、必要な時と場所で利用できるようにしておく(可用性)、の三要素を、バランスよく維持管理することを目的としたマネジメントシステムです。

国際的な第三者認証制度で、第三者の認証機関が組織のマネジメントシステムを審査し、適合した場合にその組織を認証します。当社は、2006 年に一般財団法人日本情報経済社会推進協会(JIPDEC)より認証機関としての認定を受けております。

ISMS 導入のメリット

情報セキュリティマネジメントシステムを導入することにより、以下の効果が期待できます。

- 情報資産やリスクの見える化
  多様化・高度化・複雑化する情報セキュリティのリスクに対し、経営陣の積極的な関与が可能になります。情報資産の重要度が明確になり、情報システムへの対策と経営資源の配分、方針に基づいた事業運営の効率性・安全性の向上が期待できます。

- 企業のイメージアップ
  ISMS の構築により、経営者のセキュリティに対する姿勢が評価されるとともに、営業活動や入札等への有利性、第三者認証による企業の信頼性向上が期待できます。

- 情報セキュリティ意識の向上
  ISMS の運用により、技術面だけでなく運用管理を含めた総合的なセキュリティ対策の実現が可能になるとともに、企業内のセキュリティ意識の向上が図れます。

- コンプライアンスの徹底
  ISMSの管理を通じて関連法規を認識、順守することにより、個人情報保護法をはじめとした法令順守の仕組みが整備されます。

当社の審査の特徴

1. 規格の適合性に軸足をおく厳正・適確な審査

社会環境の変化に伴い、製品・サービス・プロセス等は常に変化します。長年認証を継続している組織でも、これらの変化への対応について、その適合性を審査することが必要です。

2. 組織の特性を考慮し有効性を重視する審査

審査の結果は、単に適合の確認だけにとどまるのではなく、組織が ISO 規格に何を求めているかを尊重し、業界特性や組織文化、事業規模やシステムの成熟度など、組織の特性と個性に応じた審査をします。

3. 組織の運用実態を十分把握した審査

現場審査を重視し、トップの方針が管理部門から現場まで一貫性を持って浸透しているかを検証し、組織の方々のモチベーションを意識した審査をします。

4. コミュニケーションを重視した対話型審査

現場審査はもとより、審査の準備段階から結果報告まで、組織とのコミュニケーションにより、十分に納得いただける対話型審査を行います。こうした対話が“気づき”につながると考えています。

5. ステークホルダーの視点に立った審査

ステークホルダーの視点に立ち、「誰のため」、「何のため」に役立つシステムであるべきかを常に考えた審査を目指します。

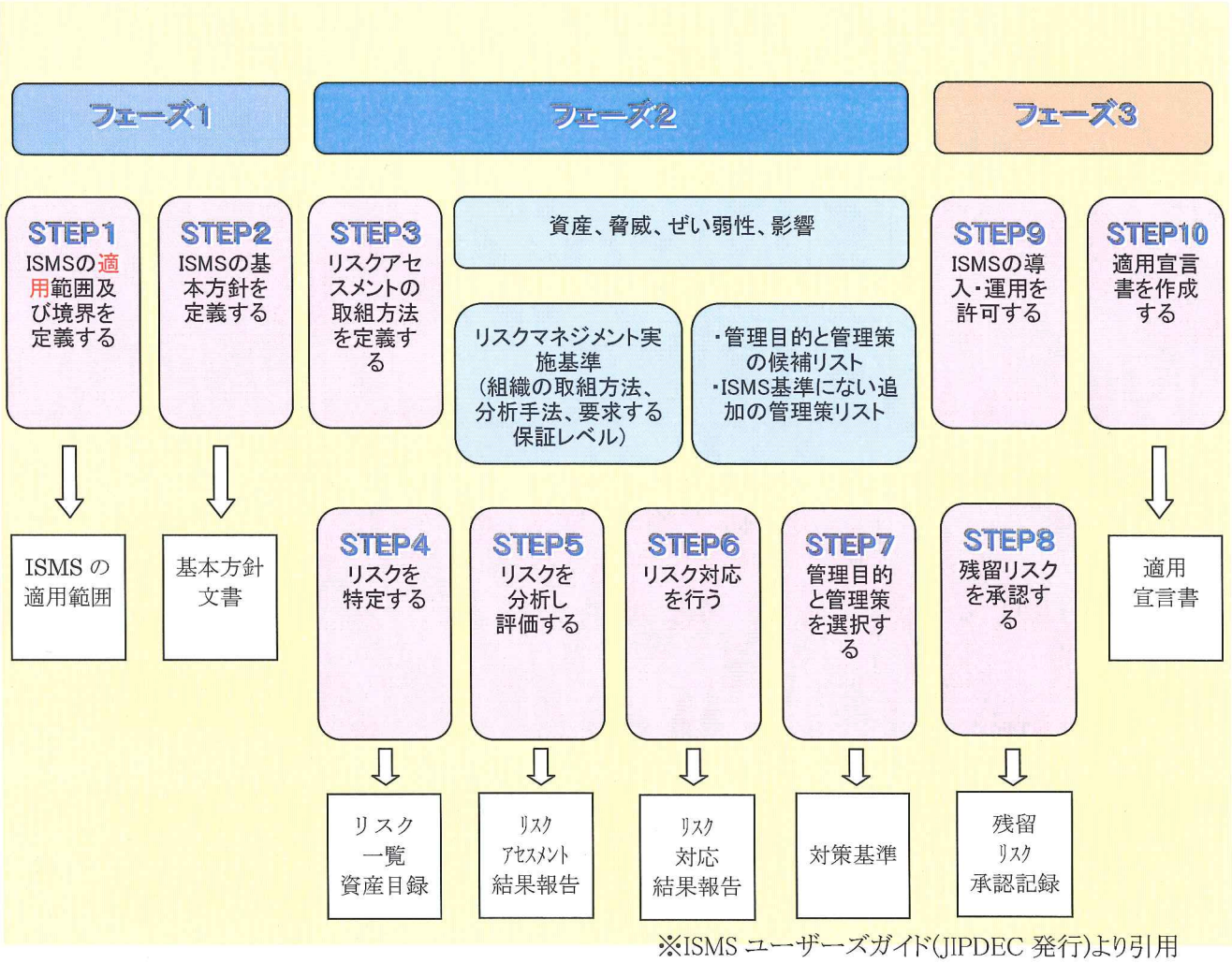
2013.11.01

日本海事検定キューエイ株式会社
〒108-0023 東京都港区芝浦3-8-10 MA芝浦ビル7階
TEL：03-5427-2505㈹ FAX：03-5427-6307
E-mail：nkqa@nkkkqa.co.jp

NKKKQA

NKKKQA

ISMSの構築ステップ



※ISMS ユーザーズガイド(JIPDEC 発行)より引用

フェーズ1： ISMS の適用範囲及び基本方針の確立
ISMS の適用範囲及び境界は、事業・組織・所在地・資産及び技術の特徴の見地から定義する。
ISMSの基本方針は、事業上及び法令又は規制の要求事項やリスクアセスメントなどから導かれる情報セキュリティに対する要求事項を考慮し、戦略的なリスクマネジメント状況、ISMSを確立し維持する。
組織環境、情報セキュリティの全般的な方向性及び行動指針を確立する。

フェーズ2： リスクアセスメントに基づき管理策を選択
決定したISMSの適用範囲・境界及び基本方針に基づき、リスクアセスメントの取組方法を特定する。
リスクの特定では、保護すべき資産に対して機密性、完全性、可用性を喪失させる脅威、ぜい弱性及びそれらが事業に及ぼす潜在的な影響の大きさを特定する。
リスクアセスメントでは、セキュリティ障害による事業上の損害及び発生可能性を評価した結果でリスクのレベルを算定し、リスク受容基準を使用して、そのリスクが受容できるか、リスク対応が必要かどうか判定する。リスクを受容できない場合、リスク対応として、管理策の適用、リスク回避、リスク移転の選択をする。リスク対応の結論に従って、附属書A「管理目的及び管理策」の表から、適切な管理目的と管理策を選択する。また、組織の必要に応じて追加の管理目的と管理策を採用することもできる。

フェーズ3： リスクに対し適切に対応する計画を策定
経営陣は、選択した管理目的及び管理策についての残留リスクを承認し、ISMSを実施する許可を与える。
選択した管理目的及び管理策並びに選択の理由と除外の理由を記載した適用宣言書を作成する。

2013.11.01

日本海事検定キューエイ株式会社
〒108-0023 東京都港区芝浦3-8-10 MA芝浦ビル7階
TEL：03-5427-2505㈹ FAX：03-5427-6307
E-mail：nkqa@nkkkqa.co.jp

NKKKQA