ＩＳＭＳコンサルティングのご提案

ＩＳＭＳとはInformation Security Management System の略で、情報セキュリティマネジメントシステムを意味します。 自社の経営に不可欠な「情報資産」を、内外の脅威から守り、リスクを低減させることを目的にしたマネジメントシステムであり、国際標準として、ISO27001が制定されており、ＩＳＭＳが定義されています。

ＩＳＭＳ（情報セキュリティマネジメントシステム）とは何か？

ＩＳＭＳ は、組織が保護すべき情報資産について機密性・完全性・可用性（CIA）をバランスよく維持し改善することを実現する為のツールです。

- 機密性（Confidentiality）：アクセスを許可された者だけが情報に確実にアクセスできること
- 完全性（Integrity）：情報資産が生成・更新・保管にわたって完全な状態で保管され、内容が正確であること
- 可用性（Availability）：情報資産が必要になったとき、利用できる状態にあること

ＩＳＭＳの基本は、ＰＤＣＡ（PLAN・DO・CHECK・ACTION）です。
確立、導入、運用・監視、見直し、維持、そして有効に機能させるための全体をＰＤＣＡによって実現します。

現代の企業経営に必要不可欠な要素であることは、誰の目にも理解できます。しかし、ＩＳＭＳは目に見えないリスクの全体像でもあり、標準に基づくシステムの構築は、有益なのです。

ＩＳＭＳをご提案する理由とTNPの強み

【お客様の目的】
自社の経営に不可欠な「情報資産」を内外の脅威から守り、リスクを低減させるマネジメントシステムの構築

【お客様の悩み】

- 運用はしているものの、「真剣にやらなくても問題は起こらない」
- 過去に検討したが、「膨大な文書化は身の丈に合わないので中断した」
- これから検討したいが、「何をどこまで対応すれば正解か分からない」

TNPの　コンサルティングを選ぶ理由

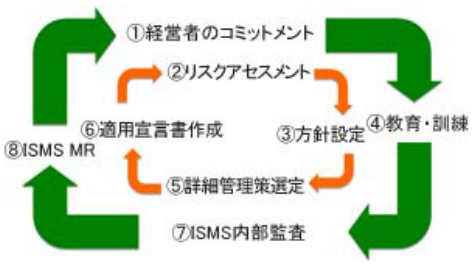
当事者が納得できる、事業の本当のリスク（価値）から導かれるＩＴリスクに対応できる
そのため、短期間、低価格で、維持継続可能なマネジメントシステムの構築ができる
目的をもった運用と改善を継続できるので、審査時期を選ばない

ＩＳＭＳを身の丈に合ったものにする

一般的なＩＳＭＳ の構築は、大量の文書化であると解釈されています。 また、ＩＳＭＳの順守を求める顧客も、形式を尊重するあまり、それを求めることがあるようです。 このようなＩＳＭＳは、運用段階に入ると、自分たちの業務に本当に必要なルールなのか、という本質的な疑問に行き当たり、上手く機能しません。 つまり、身の丈に合わない為に、そのルール守る必要があるのかを、経営者層、管理者層、担当者層のいずれもが説明できない状態に陥ってしまうのです。

ＩＳＭＳ構築コンサルティングの全体像

- 「事業リスク」を切り口にＩＴリスクを抽出、評価する独自のリスクアプローチ手法
- 多人数参加型のリスクアセスメントによる現状分析・理解によるプロジェクトの進行
- 経営層がすべてのステークホルダーに説明できる無駄のない社内基準と、文書化の支援
- 持続可能なマネジメントシステムの構築・運用・定着に向けた管理者教育的なコンサルティング内容



他のリスクアセスメントとの違い

当社のリスクアセスメントは、一般的なＩＳＭＳ のためのリスクアセスメントが入り込まない、 事業の本当のリスク（価値）から導かれるＩＴリスクを対象とする「Benefit R esource R eview 」という方法を用いるため、 ＩＳＭＳが取り扱うＩＴリスクが特別なものではないことを理解することができます。この時点で、構築後の「腑に落ちない」を解決し、維持継続の可能なマネジメントシステムとして、ＩＳＭＳを構築していきます。

一般的なリスクアセスメント	TNPのリスクアセスメントの特徴 Benefit R esource R eview
外部での事例や手法を基準（リスクを外部の事例に合わせて洗い出す）	利害関係者から求められるリスクから導く内部基準（既に存在するリスクを再確認する）
分かりやすいが当事者に実感のない（災害、作業上のミス等）ＩＴリスク	当事者が納得できる、事業の本当のリスク（価値）から導かれるＩＴリスク
膨大かつ詳細な情報資産洗い出しとリスクアセスメント	上記リスクに特化したリスクアセスメント
（膨大な文書化）	（上記リスクに特化した文書化。短期間・低価格なマネジメントシステム構築支援）

ＩＳＭＳコンサルティング内容

	No.	コンサルティング項目	概要
事前の確認		事前準備	貴社ビジネス、ＩＳＭＳ対象可能性のある範囲とその現状を事前に概観・検討します。
		• 貴社組織一般情報（ビジネスに関するパンフレット、組織図、人員構成） • 関連規制、法令の要求事項 • 拠点、臨時拠点、オフィスレイアウト図、設備配置図、ネットワーク図 • 情報セキュリティ関連文書の整備状況 • 外部委託の状況	
第一回	①	経営者のコミットメント	経営者にＩＳＭＳの本質を理解してもらうというコンサルティングであり、終了時には、ＩＳＭＳの目的、リスク管理との関係を理解していただきます。
		• ＩＳＭＳ組織体制 • 責任者決定 • 適用事業範囲案、方針案の作成	
第二回	②	リスクアセスメント	事業リスク→ITリスクという形式を用い、ITリスクが孤立したものでないことの理解を促進すると共に、取り組むべきリスクを確定していきます。 ※どこにもないリスクアセスメントを提供します。
		• リスクアセスメントの結果を熟考してもらうことで、社内にＩＳＭＳの方向性を植え付けてもらいます。 • ＩＳＭＳのコンサルティングとして行いますが、リスクアセスメントのフェーズで、事業リスクを直視してもらうことで、他の業務改善への足がかりをつくります。	
第三回	③	方針設定	暫く間をおいて方針の設定を行います。ここはプロジェクトメンバーを中心に行います。マネジメントシステムというものの本質を理解してもらい、情報セキュリティマネジメントシステムの骨格を構築します。
		• ここではじめてマネジメントに必要な文書を確定します。 • マネジメントサイクルもここで確定します。 • 情報セキュリティの目的意識をプロジェクトメンバー間で統一します。	
第四回	④	教育訓練	外部コンサルタントとして、ＩＳＭＳ運用上のポイントを全社対象に行います。基本的に管理職を中心としたウォークスルーで行います。
		• ③までをしっかり伝え、定着させるという意識改革のフェーズであり、最近のコンサルティングが弱い部分であり、ここが特徴となります。	
第五回	⑤	詳細管理策の選定	管理の目的はリスクへの対応です。管理目的に適した詳細管理策を選定します。
		• 詳細管理策の文書化を行います。	
	⑥	適用宣言書の作成	
		• 情報セキュリティマネジメントに関連して適用する管理目的及び管理策を記述します。	
結果のみ頂き確認	⑦	内部監査	マネジメントシステムの監視の役割を確立します。またＩＳＭＳの要求に対する関係者の理解を深め、かつここまでに構築したマネジメントシステムを改善します。
		• マネジメントシステムの実施状況を評価し、その結果を見直しのために経営者へ報告します。 • 監査結果に基づいた是正活動の支援もおこないます。 • ISO27001の認定申請を控えた企業に向けて、ＩＳＭＳ文書の精度アップや運用レベルの適正化を行います。	
	⑧	マネジメントレビュー	ＩＳＭＳの継続的な改善を達成するために、経営者によるマネジメントレビューを実施し、次なる活動のトリガーとします。
		• 是正処置及び予防処置を決定します。 • 必要ならば情報セキュリティポリシー及び目標、並びにセキュリティ管理策を見直します。	

ＩＳＭＳコンサルティング留意点と費用

■コンサルティングの単位

コンサルティングの単位は、特定一種類の事業かつ単一のISMS推進体制といたします（単位の例：システム発・保守事業、パッケージ販売・導入～維持支援事業、技術者派遣事業、オペレーション（サーバ、ネットワーク稼働の維持管理））

■コンサルティングの範囲

コンサルティングの範囲は、事前確認（当社負担）から始め、①経営者のコミットメント～⑥適用宣言書の作成までの5回とします。
⑦内部監査と⑧マネジメントレビューについては、文書の確認のみといたします

■コンサルティング価格（参考：15名程度の事業所）

コンサルティング価格は以下の通りといたします。
１５０万円～ （諸経費別途）

■オプションサービス

以下の事項については、個別具体的なご要望を打ち合わせた上で、別途、規模、所要期間、費用をご相談させていただきます。
・内部監査支援
・マネジメントレビュー支援
・適用事業領域拡大
・追加範囲（適用範囲）のＩＳＭＳ構築支援