最初にお読みください

当社のPMS取得支援について

初めて当社にお問い合わせいただいた皆様に

（有）中野ソフトウエアサービス
2019/12/12

プライバシーマーク取得に当たってすべきこと

プライバシーマークはお店のショーケースに売っているわけではありません。皆さん自身でのマネジメントシステムの構築と運用が必要です。

マネジメントシステムとは

マネジメントシステムは以下の要素で構成されます。

- 組織
  - トップマネジメントは誰が担うのか。誰がどのような職務権限が与えられいるのか
- 機能
  - プロセス（経営のリーダーシップ、計画、資源の整備、基幹プロセス、支援プロセス、統治など）ごとに誰が何をするのか
- 手順
  - プロセスを実現するための活動で個々人のばらつきを出さないための手順はどのように規定されているのか

標準的なプライバシーマーク取得の手順

規格の理解

PMSを理解するためには個人情報保護法とJISQ15001:2017は避けて通れません。

法律用語、ISO用語と揶揄されるようなわかりにくさはあるものの、一読しておくことは必要です。

当社では,簡単な査読用のチェックリストを用意しています。

まずは、一緒に読んで不安を解消してください。

この部分だけのサービス（1日コースで4万円）を提供しています。

組織状況の確認（チェックリストによる）

JISQ15001:2017は規格本文と付属書Aで構成されています。

マネジメントシステムで実施すべき監理施策は付属書Aに記載されています。

こちらもチェックリストを用意しているので読み合わせをして行きます。

管理施策ごとに

- 対応する活動をしているか
- 対応する規定文書はあるか
- 記録類を作成しているか

等を確認して行きます。これにより明文化されていない活動をあぶりだし必要な文書類や活動を明確にします。

小規模企業では内部監査やマネジメントレビューなどはしていないことが多いです。

手順とスケジュール作成

実際のコンサルタント業務はここから開始されます。

取得したい時期があれば、そこから逆算して行きます。無ければ半年程度を想定します。

基本は自社でマネジメントシステムを構築して運用します。

支援は、組織の状況によって変わります。

一ヶ月に2度ほどの訪問ですむ場合もありますし、もう少し頻度を上げた方が良い場合もあります。

個別に相談します。

業務プロセスの整理

利益を生み出す業務だけのことを指しているのではありません。

一般的にバリューチェーンを構成する要素ごとにプロセスがあります。基幹プロセスとしては企画、受注、製造、発送、支援プロセスとしては、研究、人事、財務などいくつもあります。個人情報を扱う可能性のある業務を洗い出します。

洗い出した業務ごとに、業務の統治、資源の調達、生産計画、設計開発、外部委託、実装、監視、改善などのプロセスごとに、誰がどのような役割で、どのような手順でどのように記録を作成して行くのかを整理します。表現はUMLやフローチャートの技法が役に立つでしょう。

この業務プロセスの整理をしっかり行っていないと、個人情報保護の対象情報の見落としやリスクアセスメントの欠落を招きます。

個人情報の取り扱いに関するリスクの明確化

前項で明確にした業務プロセスごとにリスクを整理します。

ただし、ハザードとリスクおよびリスク評価は別の概念なので混同しないこと。

ハザードとは、漏洩、毀損、持ち出し、不正利用、流失、紛失などの個人情報の取り扱いの状態を指します。

リスクは、そのハザードを引き起こす活動を指します。例えば、パソコンに保管する、車で書類を運搬する、郵送で書類を置くってもらうなどです。業務プロセスに対応します。

リスク評価は、起こりやすさや被害の程度（損害賠償になるのか、顧客との取引停止になるのか、謝ればすむのかなど）の組合わせで評価します。

この結果から、対策の程度（リスクを除去する、低減する、受け入れるなど）が決まります

不足文書の作成

リスク対策などが決まり、またマネジメント文書の必要性が決定されると、文書体系が明らかになります。

すでに組織として文書があるのならば無理に作成する必要性はありません。

ただし、文書などを識別するために記号を割り当てて文書管理ができるようにします。

文書の管理はJISQ15001:2017に記載されているのでこれに従うことが望ましいです。

従業員への教育・周知

マネジメントシステムが構築されたならば、これを社員に周知徹底させることが必要です。

教育計画として明確にして、全社員が自社のPMSへの理解が行われることを確実にします。

教育後にアンケートをとるほか、定期的な社内アンケートの実施なども有効です。

・個人情報の取り扱い上の注意点

・個人情報保護に関して事故が発生したときの報告手順

・記録類の作成を徹底することの重要性

・関連規定への理解

を中心に取り組むことが望ましいです。

運用と記録の保持

プライバシーマークの申請に当たっては、PMSを構築して運用したという実績が必要です。

JIPDECのサイトを確認する必要がありますが、本来の趣旨からいえば1年間の運用が必要です。

ただし、業務のサイクルが短期間で行われることや採用時期にかかっている場合などは短くてもPMSの運用の妥当性を主張することもできます。

組織の状況で検討します。

内部監査

内部監査についてはISO19001という規格要求事項があります。必ずしもこれに従う必要はありませんが、概ね下記が求められます。

・あらかじめ定められた間隔で行うこと（半年もしくは1年ごとが一般的）

・監査計画（監査の基準、監査員の割り当て、監査対象部門、監査日程）の作成

・監査記録の作成

・不適合などの指摘事項値の対応

・責任者への報告

JISQ15001:2017本文に記載されているのでこれに従います。小規模企業にあっては自部門の監査ができないことや経営者審査の実施の有無の判断など難しい側面があります。

内部監査での指摘への対応

内部監査で指摘された事項への対応が必要です。

一般的には、

・修正

・原因の特定

・再発防止策の策定と実施

・有効性評価

がセットになります。このあたりもJISQ15001:2017本文の「是正処置」に対応するので仕組みかしておくことが必要です。

マネジメントレビュー

マネジメントシステムの運用の適切性を評価するプロセスがマネジメントレビューになります。

言葉として「マネジメントレビュー」という用語を使わなくても良いですが、一定期間ごとに組織のマネジメントシステムが有効に機能しているのかを振り返ることが求められています。

形式的に会議体でなくても良いです。例えば、経営者の年頭挨拶で、昨年度の内部監査の結果や諸処の事件事故の経緯、経営環境の変化などに対しての対応などを配慮して行われるのであればこれをマネジメントレビューとしても良いはずです。

詳しくはISO9001の本文に記載があります。

マネジメントシステムの改善

マネジメントレビューでPMSに改善の必要性が明らかになったら、之に対処します。

一般的にはマネジメントレビューの結果や、個人情報保護に係わる事件事故などを契機に
文書類の見直しやプロセスの見直しが行われます。

こうしたプロセスの見直しもPMSに組み込んでおく必要があります。

申請書類の準備

申請書類で何が必要になるかは、JIPDECのサイトを確認します。

申請・現地調査への供え

申請を行うと、受領の知らせとともに現地調査の案内が来るはずです。

現地調査は受けたことがないと不安になり、コンサルタントなどは疑似審査などという名称でシミュレーションをすることがありますが、あまり要らないです。

最初の審査なので、マニュアル類に基づいて活動しているか、その記録はどこにあるのかなどが審査の中核になるはずです。

ここまでの対応を組織自身が行っていれば不安になる必要は無く、何もする必要は無いでしょう。

なお、現地調査にはコンサルタントの同席は認めないのが一般的なので確認してください。

指摘事項への対応

現地審査では、時々「不適合を出すことが審査員の勤めだ」という気概で審査を行う人がいます。

こうした人は、規格を自分で解釈し、組織にできそうもない対策を要求してくる人もいます。その場合は、具体的な規格の対応箇所とそれを裏付ける事実を確認し、受け入れられない場合はJIPDECに苦情を出すことを伝えると良いでしょう。

そうしないと、PMSが過剰になり運営に無理が出てしまいます。

とはいえ、企業の責任として当然と受け入れられることは対応します。

多くは、規定類の直しやリスクの見落としなどへの対応でしょう。

このやりとりは数回続くこともあるので取得したい日程が決まっているときには注意してください。

なお、コンサルタントは、この苦情に対して係わることはできないのであわせて注意してください。

当社できることとできないこと

当社にお問い合わせをいただく前にご確認ください

ご期待に添えない場合があります

私は「気が利いた作業員」ではありません。自社で人手が足りないので代行がほしいというお客様は、そうしたサービスを提供する事業所もあるので早めにお探しください。

当社のコンセプトは「山岳ガイド」に近いかもしれません。

初めてのことで、何をどう準備して良いかわからない。山頂までのルートがわからない。というお客様に、必要な知識や技術、取得工程の案内を行います。したがって、例えば山登りであれば、登山のための体力作り、パーティの構築、資材の準備、そして実際に山に登るのはお客様です。これを助けるのが当社です。

お客様自身がしなければならないこと

（1）必要文書の獲得

JISQ15001:2017を購入すること。個人情報保護法を公式サイトから入手しておくこと。JIPDECから認証取得に関する情報を取得しておくこと。

（2）具体的な手順書の作成

作成すべき文書種類の提示や雛形の提示はしますが、自社に合わせて記述するのは御社です。

（3）具体的な登録作業

JIPDECに書類を提出するなどの事務手続きはお客様の責務でお願いします。

（4）内部監査及び現地審査の対応

建前上は、外部コンサルタントが同席することは望ましくありません。

お客様への要望

「自分たちでマネジメントシステムを構築する」覚悟をお持ちください。

マネジメントシステムは「目的を達成するための、組織構造と機能を満たすための人の責任と権限、そして活動を確実に進めるための手順書」で構成されます。この時、文書作成などをすべてコンサルタントの言いなりになって作ってしまうと

- 自分たちで知らないルールが記載されていることに気がつかない
- 過剰な枠組みになってしまう（組織規模に合わない）
- 現地審査などで矛盾を指摘されても修正できない
- 経営環境が変わったときに文書のメンテナンスができない

と言ったことに陥ります。まずはご自分で作り上げて行くという覚悟をお持ち下さい。

費用の積算について

コンサルタント業務ですので、原則　10万円／日　です。

ただし、実態としては下記の通りです。

①　最初の個人情報保護法とJISQ15001:2017本文の査読だけであれば、一日支援で4万円で行っています。

②　一度にたくさんのことをお伝えしても消化しきれないことが経験的にわかっています。ですので,一回の訪問を半日として、週に一回訪問して月20万円という水準が標準的になります。

③　また、運用までの支援の頻度と、運用を開始して内部監査、マネジメントレビューの実施段階での頻度は異なります。運用開始してからはアドホックでの支援でもかまいません。

当社についてさらに知りたい場合

下記URLにアクセスしてください。

http://nss.watson.jp/