連載

使いこなして何ぼ!!のISO

…ISOコンサルティングの現場から…

第47回 Pマーク内部監査ってどうやるの????

㈱ソフィア　平松　徹

1. Pマーク内部監査の情報は貴重

Pマークの内部監査についてよく聞かれます。Pマークに関する本を読んでもよくわからないし、ISOの専門雑誌にもあまり書かれていません。しかし、外部審査のときにはかなりポイントになります。だから、情報としてかなり必要とされていることは間違いありません。

私は品質や環境ISOの審査員ですが、Pマークについては審査員補の資格も持っていません。ただ、今までのPマークの認証取得のコンサル経験から得たもので、内部監査についてもある程度確証のある仕組みを作って、企業の指導をしています。

Pマークと品質、環境ISOとの認証取得の違いは、品質、環境に比べてPマーク審査員の審査では審査員によるバラツキが大きいことが上げられます。だから、今回の私の記事をご覧になりその通りに実行した場合に、すべて適合でOK、審査にバッチリ合格するとはいかないかもしれません。

しかし、JIS Q 15001の要求事項は満たしておりますので、大きな不適合は出ないと思います。逆に、納得できる指摘であれば、それを改善の機会として活用することでうまく使いこなすということも大切です。

2. プライバシーマニュアルの例

私の作成したプライバシーマニュアルのモデルを載せます(表1参照)。基本的な構成はJIS Q 15001の要求事項とそれに対する組織の取り組みとの内容になっています。

3. 内部監査の計画文書「内部監査プログラム」の例

次に内部監査の計画文書である「内部監査プログラム」のモデルを載せておきます。参考にして

表1　プライバシーマニュアルモデル(内部監査の部分)

3.7.2　監査

JISQ15001 要求事項	責任者
PMSの 15001 規格への適合状況、PMSの運用状況を定期的に監査する。	個人情報保護監査責任者
社長は、公平、かつ客観的な立場にある個人情報保護監査責任者を社内の中から指名し、監査の実施、報告についての責任及び権限を他の責任に関わりなく与え、業務を行わせる。	
個人情報監査責任者は監査を指揮し、監査報告書を作成し、社長に報告すること。監査人の選定、監査の実施においては監査の客観性、公平性を確保する。	
監査の計画、実施、結果の報告とこれらの記録の保持に関する責任、権限を定める手順を確立し、実施し、維持する。	

当社の取り組み･･･「内部監査の手順」

項目	内容
1.目的	1)内部監査の次のことを監査する。 ・PMSが 15001 規格に適合しているか(適合性監査…主に文書監査) ・PMSが決められたとおり実行されているか(運用監査)
2.個人情報保護監査責任者	1)社長は、個人情報保護監査責任者を会社内部のものの中から指名する。 2)個人情報保護監査責任者は、社内における他の責任とかかわりなく、内部監査についての実施と報告について、権限と責任を持つ。 3) 個人情報保護監査責任者は内部監査を指揮し、監査報告書を作成し、社長に報告する。
3. 実施時期	1)原則として毎年 3 月及び個人情報保護監査責任者が必要と認めたときに実施する。
4.監査チームの決定	1)監査チーム　→　主任監査員と監査員（原則２名） ・・・個人情報保護監査責任者が内部監査員有資格者(外部監査員含む)の中から選定する。 2)監査員　→　自己の責任にかかわる部署及び自己の直接かかわる部署は監査できない。

ください(表2参照)。

4. Pマークでは内部監査を適合性監査、運用監査の2つに考えている

Pマークでは内部監査を適合性監査、運用監査の2つに考えています。上記の手順書にも入れていますが、

・PMSが15001規格に適合しているか(適合性監査…主に文書監査)
・PMSが決められたとおり実行されているか(運用監査)

の2つです。品質ISOや環境ISOでは、初回登録の審査では1次審査のときにISOの整備状況を文書の構築状況も含め審査します。Pマークでは、文書審査を適合性審査といい、運用審査と分けます。運用審査の中で文書以外の仕組みや計画の整備状況を監査します。

5. 「チェックリスト」「内部監査報告書」の例

「チェックリスト」をどのように作るかが大きなポイントになります。私の作ったモデルを「内部監査報告書」のモデルと一緒に載せておきますます。参考にしてください(表3、表4参照)。

6. Pマーク制度は規制の側面が強い

Pマーク制度は規制の側面が

5.監査プログラム	1) 年間計画 個人情報保護監査責任者は年度初めのMRで内部監査の実施時期と監査のポイントについて明確にし、マネジメント記事録に記録する。 2) 個別計画 個人情報保護監査責任者は内部監査の目的、日時、場所等の詳細を「内部監査プログラム」に明記し、関係者に通知する。
6.事前準備	1)個人情報保護監査責任者は内部監査前の会議で「内部監査プログラム」を配付し、ポイントを説明する。 2)監査員は、担当する部署の監査の範囲については事前に該当するプライバシーマニュアル、手順書・規程類の該当する箇所について目を通しておく。 3)被監査部署の責任者はプライバシーマニュアル、手順書・規程手類及び記録について再度確認しておく。
7.監査実施	(1)適合性監査(文書監査) 1) 監査員は「プライバシーマニュアル」、「手順書・規程類」、「記録様式」がJISQ15001に適合しているかどうか監査をする。 2)内部監査チェックリストに、その結果を記録する。
	(2)運用監査 1)監査員は、「内部監査チェックリスト」の項目に基づき質問をする。 ①「個人情報特定台帳」「リスク対策表」が、「プライバシーマニュアル」「手順書・規程類」に基づき作成されているか、内容が妥当であるかを確認する。 ②運用記録を確認し、実施状況を質問する。 ③実際の業務プロセスがどのように運営されているかを確認する。 ④運用の事実の要点、気付いたことを「内部監査チェックリスト」に記録する。
8.終了ミーティング	1)個人情報保護監査責任者が主催する。 2)内部監査員は、「内部監査報告書」について記述できる部分のみ作成し、ミーティングに提出する。 3) 内部監査員は「内部監査報告書」について説明し、被監査部門の責任者に対して、検討課題の原因と取るべき処置の内容について報告するよう指示をする。監査責任者は、そのときに「誰が」「いつまでに」「誰に」提出するかを明確にする。
9.具体策の実施	1)被監査部門の責任者は、不適合の原因、再発防止策などを検討し、速やかに実施する。 2)その結果については「内部監査報告書」に記録する。
10.フォローアップ	1) 改善実施の状況は、内部監査の後に実施するマネジメントレビュー又は次の内部監査で確認をする。 2) 個人情報保護監査責任者は「監査報告書」を完成し、社長及び個人情報管理責任者に提出し、報告する。 3)社長は内部監査のフォローアップの状況を確認し、「マネジメントレビュー」に記録する。 4)社長は処置の状況について、さらに是正、改善などが必要な場合、個人情報管理責任者と被監査部門責任者に新たな是正処置を指示する。

表2 内部監査プログラムのモデル

項目	内容
監査の目的	・ 構築したプライバシーマネジメントシステムのJISQ15001に対する適合性の確認(PM、手順書規程類、様式類などを確認) ・プライバシーマネジメントシステムが適切に運用されているかどうかの確認(体制整備状況、運用状況)
監査予定月日	平成 年 月 日( ) 10:00～17:00
監査対象	
監査会場	
監査チーム	監査リーダー 監査員
監査基準	適合の状況 → ＪＩＳＱ１５００１ 運用の状況 → プイバシーマニュアル、手順書・規程類
適用規格	ＪＩＳＱ１５００１

監査時間割

時間	監査員	内容、監査部署など

表3　内部監査チェックリストのモデル

内部監査チェックリスト

実施月日　　被監査部署

運用内部監査

監査員

JISQ15001 要求事項	確認文書 記録	確認内容	監査記録
3.2 個人情報保護方針	・PM ・ホームページ	・ホームページの個人情報保護方針は適切か ・周知はどのようになされているか ・PMとホームページの内容は同じか	
3.3.1 個人情報の特定	PM	どのような仕組みになっているかを確認する	

表4　内部監査報告書のモデル

内部監査報告書

承認	審査	作成

項番	項目	判定	課題など	原因	決定事項など
3.3.4	資源、役割、責任及び権限				
3.3.6	計画書				

強いことに留意する必要があります。JIS Q 15001でも「3.4.5教育」のところで「個人情報マネジメントシステムに違反した際に予想される結果」とありますし、「3.3.5内部規程」のところにも「内部規程の違反に関する罰則の規定」とあります。心理学でいうとマグレガーのX理論や、また考え方としては性悪説を基本にしているようです。だから元が善ではないので正しさを立証することに重きがおかれます。形で立証しますので、取り組みが形式的になることは否めません。Pマークを使うことを許可する以上、それを保証する文書や記録、その結果の高度なセキュリティが要求されます。コンプライアンス系の規格ですから、審査に柔軟性が乏しいのは致し方ないのかもしれません。

7.　内部監査をうまく使うことです

内部監査ではリスク対策をどのように実行しているか、それをどのように改善につなげていくかがポイントになります。リスクマネジメントということです。

また、監査を定期的なルールの確認の場にしても良いとも思います。例えばUSBメモリーを確実に保管しているかどうかの確認を内部監査で実施するなどです。日常的な運用管理だけでなく定期的な運用管理も仕組みとして要求されていますので、定期的な運用確認が必要なものについて内部監査で確認することも有効ですね。

筆　者
平松 徹(ひらまつ とおる)
中小企業診断士　環境、品質ISO主任審査員
(HP→ソフィア　平松徹→検索)