

2023年11月29日号
今年度ISO外部監査について

1分でわかる！
会社を成長させるための
桑原事務所メルマガ通信

みなさま、おはようございます。
桑原事務所の市原でございます。
今回は、ISO外部監査についてご紹介します。

この度弊所では、ISO27001 情報セキュリティ外部監査を受けました。ISOは認証内部監査でリスク（例えば情報漏洩のリスクがないか）を洗い出し、その後外部の機関が外部の目で監査を行います。外部の機関が監査を行うことで、ISOを維持し続けていい会社かどうか判断されます。弊所でも毎年受けています。

外部監査の流れとしては、3年サイクルで、更新と維持を繰り返します。

維持審査とは「問題なく運用ができているかどうか」の確認であり、更新審査とは「ISOを取得し続けていても問題無いかどうか」など、維持審査より確認項目も多く、厳しく審査されるイメージです。

この度の審査は維持審査でしたが、維持審査と併せて、事務所が移転したこともあり移転審査も行いました。

審査の流れとしては、

- ・トップインタビュー ← 代表者の考えや経営方針などのヒアリング
 - ・ヒアリング ← この度は弊所が取り扱うシステムのサイバー攻撃対応についての質問等
 - ・現場視察 ← 建物の造りやセキュリティの確認など
 - ・ISMS全体のプロセス確認 ← ISO運用記録というものがあり、その記録の確認
 - ・給与計算、労務管理プロセスの確認 ← どのような方法でデータを受け渡しているのか等
- などを行いました。

審査員からの質問を一部分だけご紹介すると、

- ・セキュリティについて
 - ・テレワーク時のルール
 - ・災害時の対応
 - ・情報漏洩の把握
- などを聞かれました。

例えば、上記セキュリティについては、移転先で建物が新しくなっても物理的なセキュリティ対策が盤石であるか？の確認がありました。弊所の営業外の時間についてはセキュリティ会社に警備を依頼しており、営業中の人の出入りについては、所内のセキュリティルームのすべてのドアはオートロック仕様のため、弊社スタッフでなければカードキーを持ち合わせず、または暗証番号での入室が出来ないように対策をとっています。

ISOは、ルールを決め、その通りに運用できているか、リスクの把握、対応はできているかを問われます。例えば、テレワークする上で持ち出し記録を作成するとルールを決めたら、それを職員が遵守し、どのように管理しているか等です。

他にも様々な確認がありましたが、大きな指摘は無く無事審査を終えることができました。

来年は3年に1度の更新審査です。今から身の引き締まる想いです。

ご不明点等ございましたら、お気軽にお問い合わせください。
よろしく申し上げます。

社会保険労務士法人桑原事務所
〒747-0064 山口県防府市高井 1143-1
[TEL:0835-22-6706](tel:0835-22-6706)
FAX:0835-26-0023
MAIL: info@kuwasr.net
