2022 年 11 月 22 日号
リスクアセスメントとは（ISO）

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 Vol.49

みなさま、おはようございます。
社会保険労務士法人桑原事務所の市原でございます。

今回は、ISO27001（情報マネジメントシステム）のリスクアセスメントについてご紹介します。

リスクアセスメントとは、ISO に限らず一般的に用いられる言葉で、リスクをあらかじめ予測しておいて、そのリスクの予測に沿ってその発生を防止するために対策をたてる、ということです。

たとえば、安全衛生の観点では、「労災事故を防ぐ、減らすためには…」と捉えていただければ分かりやすいかもしれません。

ISO におけるリスクアセスメントとは、「特定」、「分析」、「評価」の 3 つで構成されています。
特定とはリスクを洗い出すこと、分析とはどの程度の影響、重要性があるのかを把握すること、評価とは分析結果について対応方法を検討し、判断材料を揃えておくことを言います。

では、弊所の情報マネジメントを例に実際のリスクアセスメントの工程をご案内したいと思います。

まずリスクの特定については、情報セキュリティの三大要素である機密性・可用性・完全性に沿って特定していきます。言葉が専門的になってしまいましたが、可用性のリスクとは、サーバーダウンなど。機密性のリスクとは、情報の漏洩など。完全性のリスクとは、データの入力ミスなどを指します。

次のステップの分析では、特定したリスクの特徴を踏まえ、その影響の大きさを分析・算定します。5 段階の点数を付けることで、優先順位を付けることができ、その後の対応等に役立てます。

最後の評価では、分析結果を基に、リスクの影響範囲・重要性を鑑み、リスクをどのように対処するか情報を集めるのですが、これらの工程を経て社内のリスクアセスメントは完結です。

その後、洗い出したリスクに対してリスク対応というものを行うのですが、このあたりは別の機会にご案内したいと思います。

弊所でも先日外部監査が行われました。DX 化等にともなう設備や環境が変化していくにつれ、リスクもどんどん変化していきます。私たちが日常的にスルーしているところにも、新たなリスクが潜んでいることに気づかされました。1 年ごとに内部・外部監査があるので、そのタイミングごとに見直していく事が重要だと改めて実感いたしました。

次回はその事について、できたら触れていきたいと思います。

ご不明点等ございましたら、 お気軽に当事務所までご連絡ください。
よろしくお願いします。

社会保険労務士法人桑原事務所
〒747-0801　山口県防府市駅南町 8-14
TEL:0835-22-6706
FAX:0835-26-0023
MAIL: info@kuwasr.net
