Informatiebeveiligingsmanagement op basis van ISO 27001

De nieuwe ISO 27001 norm is minder rigide en dus beter toe te passen in de praktijk, onder andere door minder dubbele omschrijvingen en is alleen gericht op Informatiebeveiliging.

Vertrouwelijke gegevens, klantgegevens, wachtwoorden, strategische informatie, persoonsgegevens personeel, contracten leveranciers, notariële aktes. Digitale data is moeilijk te beveiligen vanwege verschillende vormen en formaten. Thuiswerkers, laptops, servers, back-up schijven, emailboxen.

Procesmatige aanpak voor het vaststellen, implementeren, uitvoeren, bewaken, onderhouden en verbeteren van informatiebeveiliging op basis van een ISMS systeem.

Stappenplan:

Nulmeting; huidige status en wat is nodig

Risico analyse; op basis van beheersmaatregelen (ISO 27005)

Beoordelen op basis van;

- Vertrouwelijkheid
- Integriteit
- Beschikbaarheid

Doelstellingen bepalen om risico's terug te brengen tot aanvaardbaar niveau

Criteria bepalen voor het accepteren van de risico's

Risico's evalueren

ISMS opzetten en voorzien van een pakket met beheersmaatregelen die uit de risico analyse naar voren komt met de volgende onderdelen:

- Beleid en Scope
- Risicomanagement
- Procedures personeel
- Fysieke beveiliging
- Beveiliging apparatuur
- Beveiliging van systemen
- Beveiliging van gegevens
- Crypto grafische beheersmaatregelen
- Communicatie en medewerkers bewustzijn
- Continue verbetering
- Continuïteitsplan

Het kwaliteitssysteem en de maatregelen worden door het bedrijf opgezet, wij begeleiden.

Verklaring van toepasselijkheid wordt opgesteld door het management en is het vertrekpunt voor de uiteindelijke certificering

Interne audit en het verbeterproces; nadat ISMS is ingeregeld en de beheersmaatregelen zijn geïmplementeerd wordt dmv Plan-Do-Check-Act cyclus en de interne audits aanpassingen en verbeteringen doorgevoerd. Afspraken over waar wordt wat opgeslagen en de bijpassende procedures borgen.

Certificeringsaudit middels externe audits

Zaken die van belang zijn voor ISO 27001

Risico analyse,

Beveiliging van ruimten,

Beveiliging van apparatuur

Toegangsbeheer

Toepassen functiescheiding tav informatie (inkoper mag bv geen betalingen doen)

Back-up en beschermen van Data; wachtwoord beleid, toegankelijkheid

Beleid tijdens dienstverband en erna

Waarborgen continuïteit na uitval systemen

Als we deze zaken naar behoren hebben geregeld dan is het resultaat “license 2 operate” en dit geeft de ondernemer weer rust

Informatie veilig zonder extra veel moeite

Betere procedures

Efficiëntere werkwijze

Hogere kwaliteit van de organisatie

Commercieel belang, wij zijn goed bezig

Norm 27002 wordt gebruikt als praktische richtlijn voor het ontwerpen van informatiemanagement systemen. Wordt gezien als “code of practice” en uit de praktijk is gebleken dat dit een goede leidraad is om een ISMS systeem op te zetten.

Eigenlijk is het beter om de 9001 norm te implementeren want hiermee leert het bedrijf en de medewerkers in processen te denken en procedures te volgen. ISO 27001 is een verdieping daarvan op het specifieke onderwerp informatiebeheersing. Als men een ISO 9001 certificaat heeft is er dus ook al een Kwaliteit Management Systeem ingevoerd.