ISO 27001, the lean quality way

Beschrijving

ISO 27001 Informatiemanagement

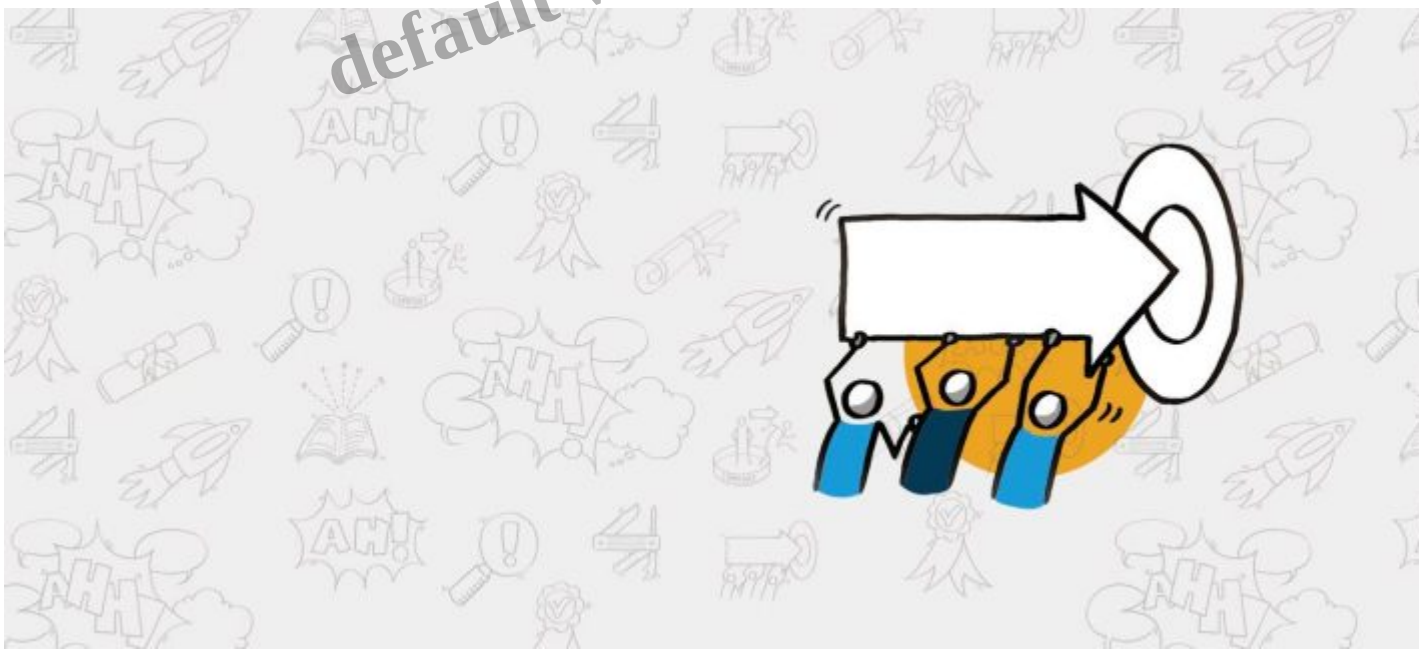
ISO 27001, veel ondernemingen en organisatie zijn hier mee bezig of overwegen hier mee aan de slag te gaan.

Vanuit onze filosofie dat kwaliteitsmanagement gewoon bedrijfsmanagement is willen we ook ISMS 27001 op een praktisch en effectieve manier organiseren.

Daarom is het goed om alvorens te starten stil te staan bij de bedoeling van deze norm en de vereiste elementen voor certificering.

Naast de verschillen gaan we ook op zoek naar de overeenkomsten tussen ISO27001 en ISO9001:2015.

Om vervolgens te kijken hoe we vanuit de overeenkomsten te komen tot een geÃ¯ntegreerd systeem.



De bedoeling van ISO 27001

Het doel van de ISMS is om de vertrouwelijkheid, integriteit en de beschikbaarheid van de informatie in een bedrijf te beschermen.

Dit kan om verschillende redenen.

Specifieke kennis en kunde van je organisatie wil je niet zomaar buiten de deur hebben.

Maar wat te denken van informatie over je klanten.

En dan hebben we het niet alleen over persoonlijke (AVG) gerelateerde data.

Toch wordt binnen veel organisaties bijvoorbeeld heel vaak (on) bewust gebruik gemaakt van â??gratisâ?• software of apps om bedrijfsprocessen te ondersteunen.

Als je informatie wilt beschermen zul je daarom ook je middelen en informatie moeten kanaliseren.

Te beginnen met het formuleren van een beleid.

Dat klinkt toch al aardig bekendâ?¦toch

Opvallende verschillen met ISO9001:2015

Wat opvalt bij het lezen van de norm is dat deze behoorlijk directief is beschreven.

ISO27001:2015 heeft (indirect) een behoorlijk aantal verplichte procedures en 114 gedefinieerde beheersmaatregelen!

We gaan een beetje terug in de tijd zoals dat bij ISO9001 in de jaren 80 ook het geval was.

Het grote gevaar hierbij is dat organisaties een ISMS tegen de normelementen gaan inrichten.

Omdat het moet. Herkenbaar?

En ja dat is jammer, want juist creativiteit en betrokkenheid van iedereen in de organisatie maakt het echte verschil.

Een tweede opmerkelijk verschil is de denkrichting.

ISO9001 gaat om het behalen van een positief procesresultaat, een service of eindproduct voor de klant met toegevoegde waarde.

Bij ISO27001 kun je eigenlijk alleen verliezen, de inzet is preventief gericht op het voorkomen van informatiebeveiligingsincidenten.

Gezien de snelheid van ICT-ontwikkelingen echter zeker noodzakelijk om dit onder controle te hebben.

ISO27001 meets ISO9001

Het is te gemakkelijk om je te beperken tot de HLS-indeling van de norm.

Het hsl-niveau van ISO27001 is heel beperkt beschreven, het werk zit echt in de maatregelen.

Maar er zijn wel degelijk meer overeenkomsten.

Denk hierbij aan de verbetercyclus en de risico gebaseerde aanpak.

Maar men kan het nog veel concreter maken.

Alle informatiebronnen, dragers of hoe je ze ook wilt noemen worden gebruikt in bedrijfsprocessen.

In het SIPOC-model is het dus gekoppeld aan de input en output, de beheers aspecten.

Hier ligt dus een kans om beide normen op een logische manier te koppelen en te integreren.

De combinatie: hoe dan?

Een bekend gezegde, er zijn meerdere wegen die naar Rome leiden.

Dit is ook van toepassing op een geÃ¯ntegreerd ISO9001 en 27001 managementsysteem.

Bij een ISO9001 project gaan we meestal aan de slag met Brown paper sessie om de processen in kaart brengen.

Deze aanpak is gestructureerd waarin we beschrijven wat we doen. Er hoeft niet buiten de bekende kaders te worden gedacht.

Bij ISO27001 kun je de aanpak echter het beste vergelijken met een FMEA of een andere risicostudie.

Vanuit een brainstorm achtige sessie worden risicoâ??s geÃ¯nventariseerd, geclassificeerd en zonodig met aanvullende maatregelen gereduceerd tot acceptabel niveau.

Hoe hoger de kwaliteit van de input uit de brainstorm, des te beter is het eindresultaat.

Met een slim digitaal kwaliteitsmanagementsysteem kan men vervolgens het resultaat borgen en eenvoudig aantoonbaar maken voor belangstellenden.

Meer weten of hulp nodig?

Wij laten vooraf zien hoe wij werken en wat het resultaat kan zijn.

Ook bij ons maakt de mens en verbinding het verschil.

Of volg de implementatie met de blogs bij deze software organisatie

Categorie

1. blog

Datum aangemaakt

2020/03/29
Auteur
anton_s