# Handleiding invoering Managementsysteem voor informatiebeveiliging op basis van de ISO 27001:2013

September 2016

## Beste Informatiebeveiligingsmanager in spé,

Het beveiligen van informatie wordt steeds belangrijker. Niet voor niets wordt het aantoonbaar hebben van werkend managementsysteem voor informatiebeveiliging door verschillende partijen (overheid, klanten) steeds meer gevraagd of geëist.
Dat vele niet licht over het opzetten van zo'n informatiebeveiligingssysteem denken blijkt wel uit de behoefte aan begeleiding die organisaties nodig hebben om een managementsysteem voor informatiebeveiliging in te richten. Je zou kunnen zeggen: het is een opkomend vakgebied. U zult merken dat met dit pakket het invoeren van een managementsysteem voor informatiebeveiliging door iedereen goed te doen is.

Omdat het vak van Informatiebeveiligingsmanager voor u waarschijnlijk nieuw is geven wij u binnen deze handleiding eerst uitleg over de opbouw en functie van het managementsysteem voor informatiebeveiliging. Ook nemen wij de ISO 27001 norm door en leggen wij u de meest belangrijke begrippen uit. Zo leert u de taal van de certificeerder spreken. De certificeerder is de vertegenwoordiger van de certificerende instelling die u aan het einde van dit proces het certificaat verstrekt.

Daarna geven wij u binnen deze handleiding alle informatie die u nodig heeft om het managementsysteem op te kunnen zetten. Denk daarbij aan het formuleren van het informatiebeveiligingsbeleid, het uitvoeren van de risicobeoordeling, het beheren van documenten, het meekrijgen van het management en nog meer. Deze handleiding eindigt met een stuk informatie over het kiezen van de juiste certificeerder en het certificatietraject.

Om u door het proces te leiden hebben wij voor u een projectplan opgesteld. Dit projectplan geeft u in een oogopslag inzicht in alles wat er dient te gebeuren. Het is de komende maanden uw houvast.

## Hoe kunt u het beste starten?

1. Start met het downloaden van alle documenten en archiveer deze op duidelijke manier binnen uw computer.

2. Lees daarna deze handleiding goed door. Het kost even tijd, maar u zult merken dat u daarna als vanzelf het systeem kunt opzetten.

3. Print daarna alle documenten uit en doe deze overzichtelijk in een map.

4. Wanneer u de helpteksten uit de documenten wilt verwijderen kan dat door met de rechtermuisknop op de helptekst te klikken en te kiezen voor: *opmerking verwijderen*.

5. Ga daarna met het projectplan aan de slag. U zult merken dat u dankzij de voorbeelden en de gevulde sjablonen snel een start kunt maken met het opstellen van het informatiebeveiligingsbeleid en het invoeren ervan. U zult in deze periode nauw samenwerken met uw management en collega's waardoor het systeem snel vorm zal krijgen.

6. Wanneer u ook VisionManager heeft aangeschaft adviseren wij u om alles wat u voor het managementsysteem produceert meteen binnen VisionManager onder te brengen. VisionManager kunt u gratis 14 dagen proberen bij www.visionmanager.nl

Mocht u nog vragen hebben kunt u altijd een mail sturen aan info@isomanager.nl.

Wij wensen u veel succes toe met de implementatie van uw managementsysteem voor informatiebeveiliging.

Team AVR Vision Consult BV

## Inhoud

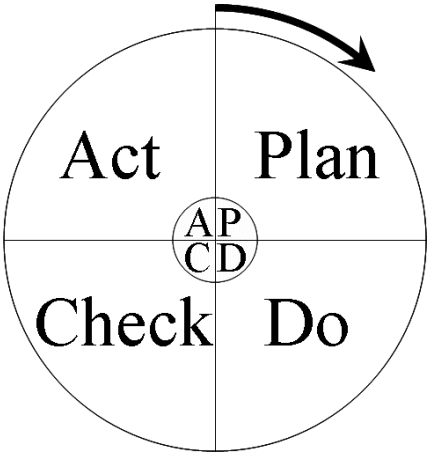
# 1. Filosofie achter de ISO 27001:2013

In dit hoofdstuk vertellen wij u in het kort wat u als Informatiebeveiligingsmanager van de ISO 27001 norm moet weten. Het belangrijkste is dat u de filosofie van de norm begrijpt. De ISO 27001 is opgebouwd rondom vier thema's:

1. Het kennen van de context van de organisatie en het informatiebeveiligingsbeleid.
2. Het kennen van de risico 's op het gebied van informatiebeveiliging.
3. Het hebben en uitvoeren van adequate borgingsmechanismes om de risico 's zo goed als nodig te beheersen.
4. Het meten van de resultaten van de borgingsmechanismes, het analyseren ervan en het zo nodig verbeteren van het managementsysteem.

Binnen thema één is het informatiebeveiligingsbeleid veruit het belangrijkst. De basis van het managementsysteem wordt gevormd door het informatiebeveiligingsbeleid.

In thema vier komt het meten, analyseren en zo nodig verbeteren aan de orde. De gebruikte systematiek is gebaseerd op de Deming Cirkel (PDCA-cirkel).




Deze systematiek wordt binnen ISO 27001 telkens weer opnieuw toegepast om verbeteringen door te voeren of doelstellingen te realiseren.

In de PLAN fase beschrijft u de benodigde acties om de oorzaak van de afwijking weg te nemen, of de benodigde acties om de doelstelling te realiseren.

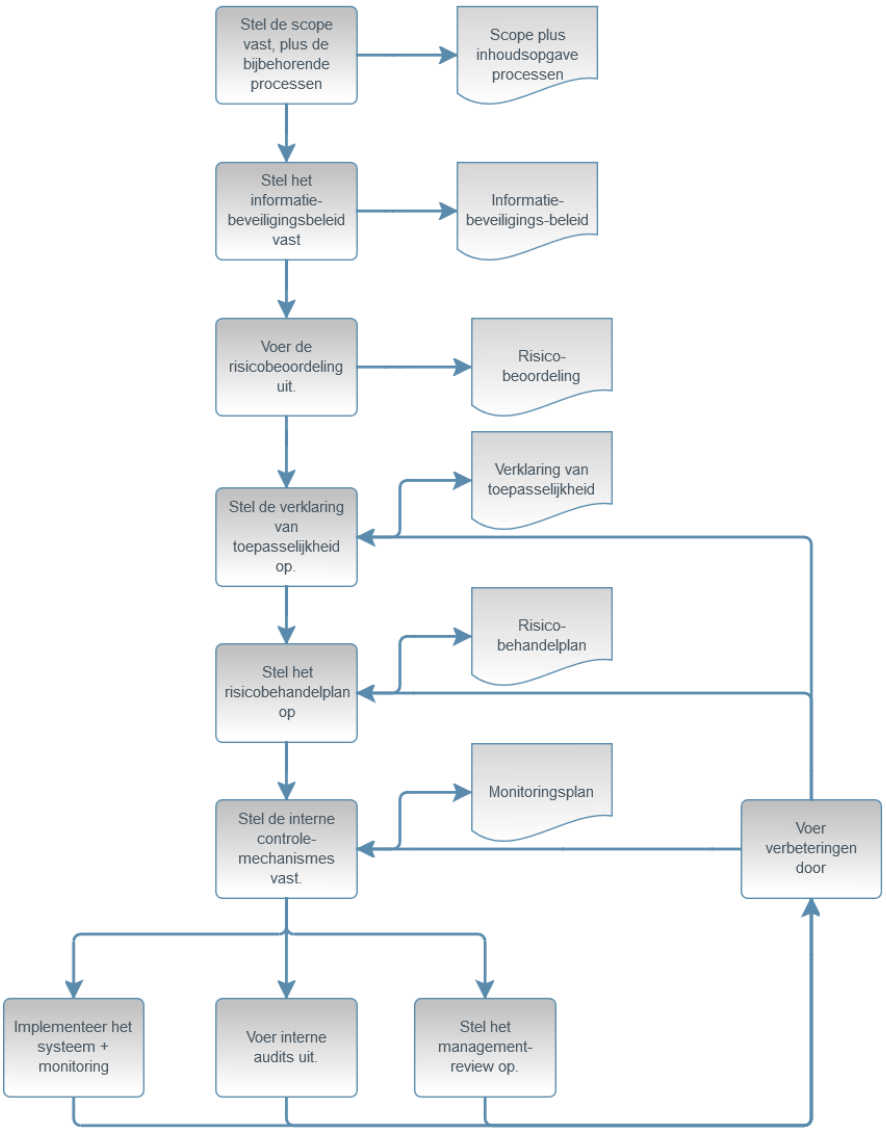
Binnen de DO fase voert u deze acties uit.

Binnen de CHECK fase controleert u of de acties tot het gewenste effect hebben geleid. Zo niet dan zult u uw plan moeten bijstellen (ACT fase). U doorloopt dan opnieuw de cirkel. Vergeet niet het behaalde resultaat te borgen!

Let er als informatiebeveiligingsmanager op dat wanneer er een verbetering wordt doorgevoerd u deze laat toetsen op effectiviteit. Dit is een aspect waar de certificeerder zeker naar zal kijken.

## 2. Dit zijn de stappen die u gaat doorlopen bij het opzetten van de ISO 27001.

Schematisch ziet het doorlopen van het ISO 27001 project er als volgt uit:




Binnen deze handleiding geven wij uitleg en tips over hoe u het beste bovenstaande stappen kunt uitvoeren. Samen met het projectplan en de templates geeft het u een goede start voor het invoeren van uw informatiebeveiligingssysteem.

# 3. De Informatiebeveiligingsmanager / Leiderschap

U hoeft volgens de ISO 27001 geen Informatiebeveiligingsmanager (of kwaliteitsmanager) aan te stellen. Het mag wel. De meeste organisaties kiezen ervoor om dit wel te doen. De Informatiebeveiligingsmanager moet dan wel lid zijn van het Management Team. Alle taken en verantwoordelijkheden die de Informatiebeveiligingsmanager heeft mogen ook worden toebedeeld aan het Management Team.

Zorg er dan wel voor dat het heel duidelijk is wie verantwoordelijk is voor wat. In de praktijk is dit niet zo gemakkelijk te regelen, en wordt er vaak gekozen om deze activiteiten toch bij een informatiebeveiligingsmanager neer te leggen.

Het gaat om de volgende taken en verantwoordelijkheden:

- Het hebben (als organisatie) van een concreet informatiebeveiligingsbeleid, met bijbehorende doelstellingen, als afgeleide van de missie, visie en kernwaarden.
- Het aantoonbaar communiceren van het informatiebeveiligingsbeleid.
- Het verwerken van de eisen binnen de processen.
- Het aantoonbaar sturen aan de hand van de realisatie van de doelen en prestaties.
- Het aantoonbaar beheersen van de daarvoor aangewezen risico's (managers moeten kunnen aangeven wat zij er aan doen om de risico's te beheersen).
- Continue verbeteringen bevorderen.
- Mensen aan te sturen en te ondersteunen.

Dit zijn lastige gebieden omdat ze veel te maken hebben met het strategisch beleid van de organisatie. Het werkt dan ook alleen wanneer de Informatiebeveiligingsmanager rechtstreeks rapporteert aan de hoogste in rang binnen de organisatie. Een goede Informatiebeveiligingsmanager is de rechterhand van de directeur / bestuurder van de organisatie.

Daarnaast is een Informatiebeveiligingsmanager onder meer verantwoordelijk voor:

- Het documentenbeheer.
- Het hebben en laten uitvoeren van de interne auditplanning.

Houdt de verantwoordelijkheden daar waar ze horen. Het merendeel blijft dus gewoon bij het management. Dat betekent dat een Informatiebeveiligingsmanager het management kan aanspreken (adviesplicht) op allerlei gebieden waar niet alle managers op zitten te

wachten. Het is verstandig om deze bevoegdheid van de Informatiebeveiligingsmanager formeel te regelen.

# 4. Het project

## 4.1 Het projectteam

Het invoeren van een managementsysteem voor informatiebeveiliging vraagt tijd en vooral aandacht. Veel organisaties kiezen ervoor om een projectteam samen te stellen die het ISO project uitvoert. Zorg ervoor dat de samenstelling van het projectteam zodanig is dat er naast medewerkers die het feitelijke projectwerk doen er ook managers in zitten die de benodigde beslissingen kunnen nemen en voor draagvlak kunnen zorgen.

## 4.2 Het projectplan

Onderdeel van het pakket is een projectplan. Hierin staan in het kort de benodigde acties aangegeven die moeten worden uitgevoerd om op een succesvolle manier het ISO systeem in te voeren. Gebruik dit projectplan als leidraad. Voor eventuele uitleg wordt vanuit dat projectplan naar deze handleiding verwezen.
Het projectplan neemt u feitelijk aan de hand om het gehele proces te kunnen doorlopen.