BIJLAGE behorende bij
ISO/IEC 27002: 2013
Grafimedia en Creatieve Industrie

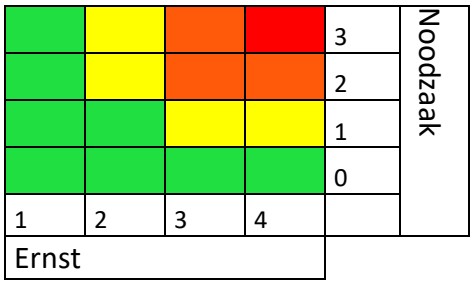
Onderdeel van de Certificatienorm Informatiebeveiliging

Uitgave van de Stichting Certificatie Grafimedia branche (SCGM)

Bijlage A: Instrument voor Risicoanalyse, het stoplicht model

Het stoplichtmodel biedt een visuele weergave van het beveiligingsniveau waardoor het mogelijk wordt om verbeteringen hiervan stapsgewijs in te voeren en zicht wordt gekregen op de status van het risicomanagement en de besluitvorming overzichtelijk wordt. Daarnaast biedt het model de mogelijkheid maatregelen direct met de betrokkenen af te stemmen en zo passende en haalbare oplossingen te vinden. De maatregelen kunnen in de tijd worden geplaatst, zodat ook een fasering in de tijd inzichtelijk kan worden gemaakt.

Stoplichtmodel



De noodzaak geeft de afhankelijkheid van de organisatie voor een bepaalde component weer, de noodzaak om dit te beveiligen. De ernst geeft de ernst van de bedreiging voor deze component weer.

Per risicogebied kunnen de risico's en de mogelijke maatregelen om deze te beperken in kaart worden gebracht en het effect daarvan worden bepaald in een verbetering van het risicoprofiel. Voor het management zullen ook de kosten die met het nemen van de maatregelen gemoeid zijn belangrijk zijn. Deze kunnen in de maatregelen tabel worden opgenomen.

#	Risicogebied	Risico	Noodzaak /Ernst nu	Maatregelen	Noodzaak /Ernst toekomst
6	Beheer van communicatie en bedieningsprocessen (ook computer en netwerkbeheer genoemd)	Er is niet duidelijk wat onder beveiligingsincidenten wordt verstaan	3.2	Voorlichting en communicatie verbeteren	3.1
		Er zijn antivirusmaatregelen genomen op servers en werkstations	3.1	OK	3.1
		Handtekening voor gebruik laptops nodig?	1.2	Reglement gebruik laptops opstellen	1.1
		Is voor alle type incidenten duidelijk wie voor de afhandeling van het incident zorg draagt	3.1	OK	3.1
		Is er voldoende personeel met de juiste expertise om te zorgen voor een tijdige oplossing van incidenten	3.1	OK	3.1
		Heeft de organisatie beleid m.b.t. het naleven van	3.1	OK	3.1

Vervolgens kan er een totaaloverzicht opgesteld worden van de risico's per risicogebied.

#	Risicogebied	Noodzaak /Ernst nu	Noodzaak /Ernst toekomst
1	Beveiligingsbeleid	3.2	3.1
2	Organisatie van informatiebeveiliging	3.3	3.2
3	Beheer en classificatie van bedrijfsmiddelen	2.2	2.1
4	Personele beveiligingseisen	3.3	3.2
5	Fysieke beveiliging en beveiliging van de omgeving	3.4	3.3
6	Beheer van communicatie en bedieningsprocessen	3.2	3.1
7	Toegangsbeveiliging	3.4	3.2
8	Ontwikkeling en onderhoud van informatiesystemen	3.2	3.2
9	Bedrijfscontinuïteitsbeheer	3.2	3.1
10	Naleving	3.2	3.1

