BIJLAGE behorende bij ISO/IEC 27002: 2013 Grafimedia

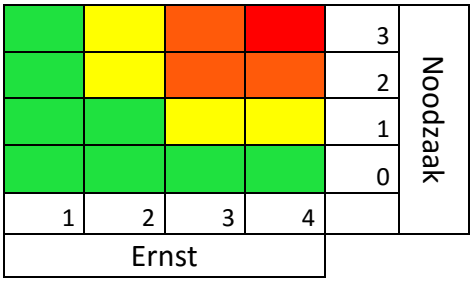
Onderdeel van de Certificatienorm Informatiebeveiliging

Uitgave van de Stichting Certificatie Creatieve Industrie (SCCI)

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.

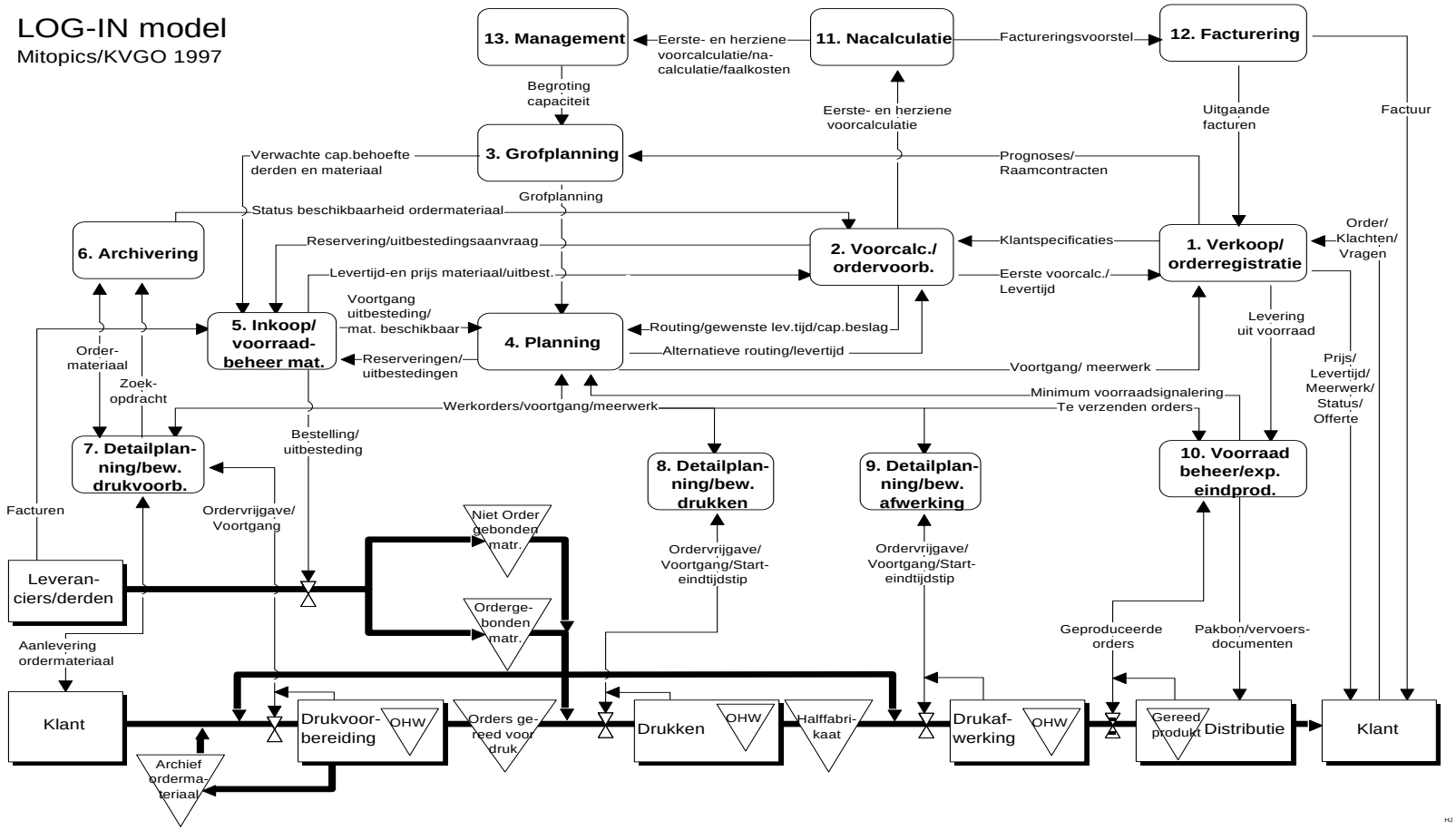
#	Risicogebied	Noodzaak /Ernst nu	Noodzaak /Ernst toekomst
1	Beveiligingsbeleid	3.2	3.1
2	Organisatie van informatiebeveiliging	3.3	3.2
3	Beheer en classificatie van bedrijfsmiddelen	2.2	2.1
4	Personele beveiligingseisen	3.3	3.2
5	Fysieke beveiliging en beveiliging van de omgeving	3.4	3.3
6	Beheer van 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

BIJLAGE B: Hoofdlijnen beleidsuitgangspunten

Hieronder is een overzicht opgenomen van onderwerpen die deel uit kunnen maken van een statuut met uitgangspunten voor informatiebeveiliging

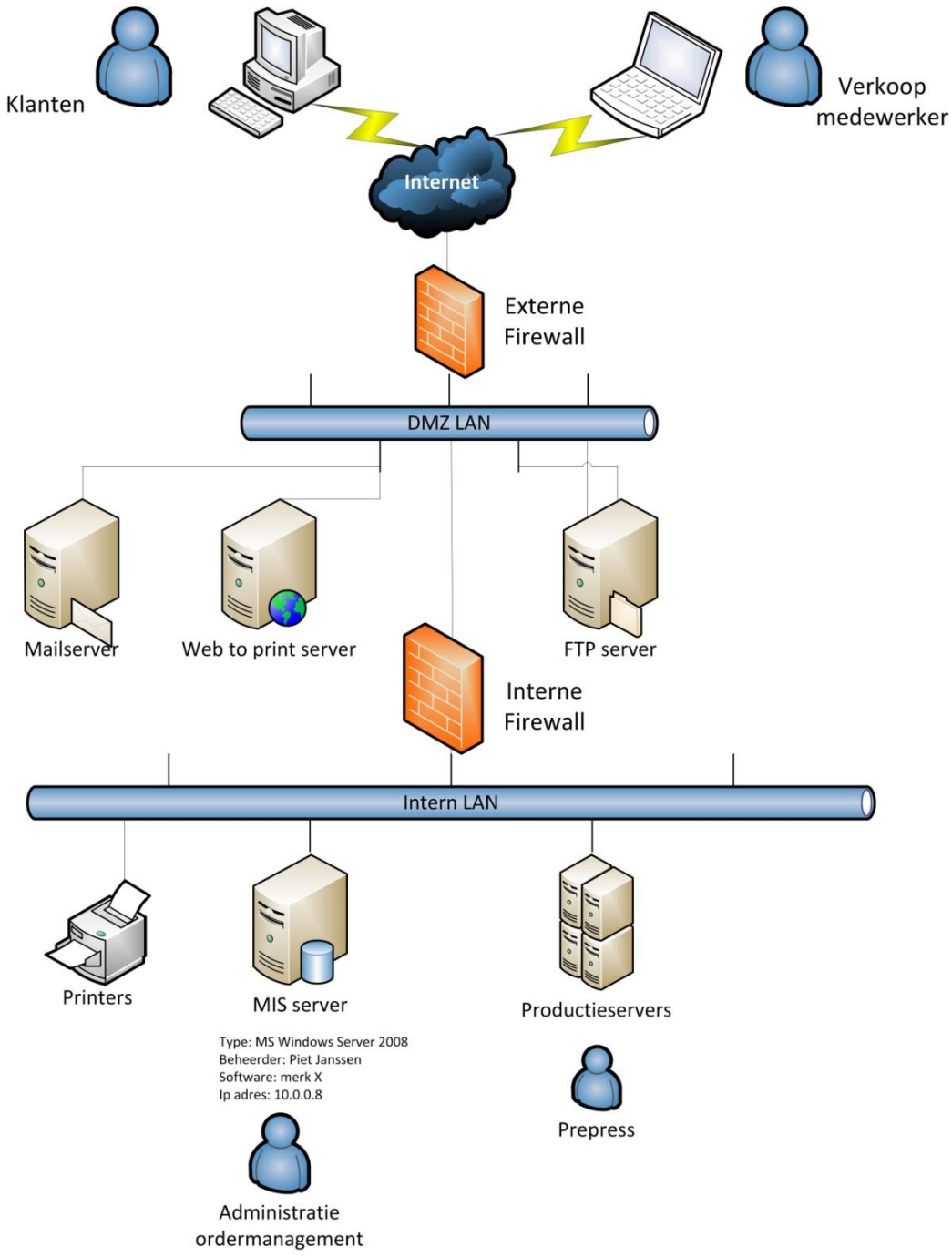
- Uitgangspunt vormen de doelstellingen van de norm NEN-ISO/IEC 27002 voor zover zij bijdragen aan de informatiebeveiliging. Als een doelstelling op een andere wijze gerealiseerd wordt via alternatieve maatregelen, dan is dat toegestaan, mits dit alternatief beschreven is.
- De fysieke en logistieke beveiliging van de computercentra en de andere bedrijfsgebouwen is zodanig, dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en gegevensverwerking gewaarborgd zijn.
- Aanschaf, installatie en onderhoud van geautomatiseerde gegevensverwerkende systemen, evenals inpassing van nieuwe technologieën, mogen geen afbreuk doen aan het niveau van veiligheid van de totale informatievoorziening.
- Het personeelsbeleid is mede gericht op het leveren van een bijdrage aan de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening.
- Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening kan ontstaan.
- Ontwikkeling van en onderhoud op informatiesystemen geschieden binnen de kaders en regels van de vastgestelde ICT-architectuur volgens een standaardmethodiek, waarbij de documentatie volgens een vaste systematiek tot stand komt.
- Bij de geautomatiseerde informatievoorziening zijn strikte scheidingen aangebracht tussen de test-/ontwikkelomgeving, de acceptatietestomgeving en de productieomgeving.
- Er zijn functiescheidingen aangebracht tussen de systeemontwikkelings-, beheer- en gebruikersorganisatie.
- Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten en personeel te waarborgen.
- Logische toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de geautomatiseerde systemen, gegevensbestanden en programmatuur.
- Gegevensverstrekking intern en extern gebeurt op basis van 'need to know'. Medewerkers treffen maatregelen om te voorkomen dat informatie in handen van personen terechtkomt, die deze informatie niet strikt nodig hebben. Ook de toegang tot informatiesystemen wordt volgens dit principe adequaat beveiligd. Voor ICT-beheerders wordt hierop een uitzondering gemaakt, om te komen tot een betere service aan de gebruikers.
- Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van de gegevens en op de informatievoorziening als geheel.
- End-user computing is omgeven door zodanige maatregelen, dat de vertrouwelijkheid en de integriteit van de opgeleverde informatie.
- Teneinde computervirusinfecties te voorkomen wordt er slechts gewerkt met geautoriseerde versies van (legale) programmatuur.
- De bescherming van digitale materialen van klanten en digitale materialen waar rechten op liggen, wordt gewaarborgd.
- Het beheer en de opslag van gegevens zijn zodanig, dat geen informatie verloren kan gaan.
- Er is een proces om incidenten adequaat af te handelen en hier 'lessons learned' uit te trekken.
- Er zijn calamiteitenplannen en -voorzieningen om de continuïteit van de bedrijfsvoering en de informatievoorziening te waarborgen en imagoschade te voorkomen.

BIJLAGE C: Voorbeeld informatiestroom diagram



BIJLAGE D: Voorbeeld systeemarchitectuur

Onderstaand is een vereenvoudigd voorbeeld van een systeemarchitectuur beschreven:



Bijlage F: Checklist voor aanschaf van Informatiesystemen

Onderwerp	Voldaan?	Opmerking
1. Beoordeling leverancier		

• Gebruikersondersteuning
  ○ Is er een helpdesk aanwezig
  ○ hoe lang is die helpdesk geopend?
  ○ Is er een calamiteitennummer met welke uren per week aanwezigheid?
• Geleverde service door leverancier (onderhoud en reactiesnelheid na incidenten)
• Liggen de afspraken over de te verwachten dienstverlening vast in een service level agreement.
• Betrouwbaarheid en reputatie leverancier (Bedrijfsomvang en reputatie, toekomstverwachting)		

2. Software		

• Geldige licenties
• Beschikbaarheid documentatie
• Compatibiliteit met bestaande omgeving
  ○ Importeren bestaande data
  ○ Bekende conflicten met bestaande software
  ○ Compatibiliteit met bestaande hardware
• Mogelijkheden om met veilige wachtwoorden te werken en gebruikers middels rollen te beheren
• Gebruik beveiligde communicatie bij gevoelige informatie		

3. Risicoafweging bij de aanschaf		

• Welke specifieke risico's loopt de nieuwe applicatie of hardware zelf?
  ○ Wisselt de applicatie gegevens uit, is de beveiliging gewaarborgd?
  ○ Wordt er informatie buiten de organisatie opgeslagen?
  ○ Natuurlijke risico's zoals verlies bij draagbare apparatuur
  ○ Beschikbaarheid van kritische applicaties en hoge vertrouwelijkheid van informatie
• Welke aanvullende maatregelen of wijzigingen op bestaande maatregelen zijn wenselijk? Moeten er nieuwe maatregelen genomen om de nieuwe aanschaf veilig te gebruiken?
• Is nadere risicoafweging door of advies van een expert nodig?		

4. Implementatie van nieuwe software, hardware en randapparatuur		
• Neem de nieuwe hardware, software of randapparatuur op in het overzicht van hardware, software en randapparatuur		