# DIRECTIE BEOORDELING 12-7-2015

De directie moet met geplande tussenpozen het managementsysteem voor informatiebeveiliging van de organisatie beoordelen, om de continue geschiktheid, adequaatheid en doeltreffendheid te bewerkstelligen. Bij de directiebeoordeling moet onder andere in overweging worden genomen:

a) de status van acties als gevolg van voorgaande directiebeoordelingen;

**Dit is de eerste directie beoordeling.**

b) wijzigingen in externe en interne onderwerpen die relevant zijn voor het managementsysteem voor informatiebeveiliging;

**Er zijn geen wijzigingen aan te wijzen gegeven het feit dat dit de eerste directie beoordeling is**

c) feedback over de informatiebeveiligingsprestaties, met inbegrip van trends in:

**De informatiebeveiligingsprestaties zijn op formeel vlak nog niet significant; er is echter duidelijk sprake van een enorme toename van belangstelling alsmede een toename van het bewustzijn rond informatiebeveiliging onder de medewerkers.**

- afwijkingen en corrigerende maatregelen;
- resultaten van monitoren en meten;
- auditresultaten; en
- voldoen aan informatiebeveiligingsdoelstellingen;

**De directie heeft geen trends geconstateerd in afwijkingen nog in corrigerende maatregelen. Er is nog te weinig informatie om trends te kunnen zien in resultaten van monitoren en meten. Er zijn nog maar enkele audits uitgevoerd. Er wordt hard gewerkt om te kunnen voldoen aan de informatie beveiligingsdoelstellingen.**

d) feedback van belanghebbenden;

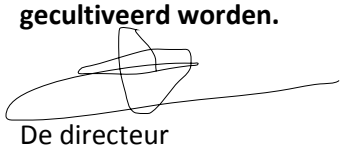
**Er is duidelijk sprake van een enorme toename van belangstelling alsmede een toename van het bewustzijn rond informatiebeveiliging onder de medewerkers; de directie ontvangt hierover positieve feedback. Er is een groot draagvlak voor het informatie beveiligings beleid.**

e) resultaten van risicobeoordeling en de status van het risicobehandelplan; en

**Uit de eerste voorlopige risico beoordelingen komt naar voren dat vooral op het gebied van bedrijf continuïteit veel te doen is. Het risicobehandelplan is niet helemaal formeel geïmplementeerd; een aantal controls moeten nog formeel omschreven worden. In de praktijk zijn de juiste mechanismes al wel operationeel.**

f) kansen voor continue verbetering.

**Het proces van continue verbetering wordt goed gedragen door het personeel. Dit moet gecultiveerd worden.**



De directeur

Rutger de Nooij

12-7-2015

## DIRECTIE BEOORDELING 27-9-2016

De directie moet met geplande tussenpozen het managementsysteem voor informatiebeveiliging van de organisatie beoordelen, om de continue geschiktheid, adequaatheid en doeltreffendheid te bewerkstelligen. Bij de directiebeoordeling moet onder andere in overweging worden genomen:

a) de status van acties als gevolg van voorgaande directiebeoordelingen;

**Dit is de tweede directie beoordeling. In de eerste directie beoordeling viel te lezen: "Uit de eerste voorlopige risico beoordelingen komt naar voren dat vooral op het gebied van bedrijf continuïteit veel te doen is. Het risicobehandelplan is niet helemaal formeel geïmplementeerd; een aantal controls moeten nog formeel omschreven worden. In de praktijk zijn de juiste mechanismes al wel operationeel."**

**Op het gebied van continuïteit wordt inmiddels gedaan wat commercieel verantwoord mogelijk is. Wel missen we nog formeel de continuïteitsplannen voor Deltacom-cloud.nl en DeltacomVOIP. Deze worden op korte termijn gemaakt. Het is wel duidelijk dat het niet mogelijk is reële operationele plannen te ontwerpen maar dat afwegingen op papier gesteld zullen worden.**

b) wijzigingen in externe en interne onderwerpen die relevant zijn voor het managementsysteem voor informatiebeveiliging;

**Er zijn geen ingrijpende wijzigingen in externe en interne onderwerpen aan te wijzen. Wel zien we dat inmiddels wetgeving actief is op het gebied van privacy en datalekken waar rekening mee moet worden gehouden.**

c) feedback over de informatiebeveiligingsprestaties, met inbegrip van trends in:

**De informatiebeveiligingsprestaties zijn goed. Het primaire proces wordt op het gebied van informatiebeveiliging volledig beheerst. Verbeteringen vinden continue en veelal "on-the-fly" plaats.**

- afwijkingen en corrigerende maatregelen;
- resultaten van monitoren en meten;
- auditresultaten; en
- voldoen aan informatiebeveiligingsdoelstellingen;

**De directie heeft geen trends geconstateerd in afwijkingen nog in corrigerende maatregelen. Het proces van monitoren, meten, auditen gaat in een zeer hoog dagelijks tempo. Het is een praktisch proces waarbij voortdurend gecommuniceerd wordt door belanghebbenden.**

d) feedback van belanghebbenden;

**De directie ontvangt steeds positieve feedback. Er is een groot draagvlak voor het informatie beveiligingsbeleid.**

e) resultaten van risicobeoordeling en de status van het risicobehandelplan; en

**We lopen achter op het gebied van formele risico analyse en risico beoordeling. De praktische kant echter functioneert in een zeer hoog dagelijks tempo.**

f) kansen voor continue verbetering.

**Er is steeds meer synergie tussen de processen Deltacom-cloud.nl en Deltacom100%. Hierin heeft Deltacom-cloud.nl een voortrekkersrol omdat informatiebeveiliging nog kritischer is en beheersmaatregelen dagelijks ontwikkeld en geïmplementeerd worden. Deltacom100% kan hier steeds beter van profiteren.**

De directeur

Rutger de Nooij

27-9-2016

DIRECTIEBEOORDELING 19-9-2017

**Dit is de derde directiebeoordeling sinds het behalen van de ISO27001 certificering. Binnen de organisatie zijn het afgelopen jaar wijzigingen doorgevoerd die betrekking hebben op de scope van onze ISO27001 certificering. Deltacom is gestopt met de directe levering van VOIP diensten in eigen beheer. Hiermee is het volledige proces van VOIP komen te vervallen. Klanten zijn overgedragen aan van den Hil telecom. Wat rest zijn de processen voor onze diensten "Deltacom100%" en "Deltacom-cloud.nl". Overwegingen op het gebied van continuïteit zijn inmiddels op papier gesteld. De synergie tussen de processen Deltacom-cloud.nl en Deltacom100% is inmiddels optimaal te noemen. "Deltacom-cloud.nl" heeft hierin nog steeds een voortrekkersrol omdat informatiebeveiliging binnen dit proces nog kritischer is en beheersmaatregelen dagelijks ontwikkeld en geïmplementeerd worden. Het proces "Deltacom100%" profiteert hier inmiddels maximaal van ook omdat binnen de beheertools en beheeromgevingen overlap is.**

**Er zijn geen zeer ingrijpende wijzigingen in externe en interne onderwerpen aan te wijzen. Wel zien we dat inmiddels wetgeving actief is op het gebied van privacy en datalekken waar rekening mee moet worden gehouden. Het ligt wel in de verwachting dat in de aanloop naar mei 2018 als de GDPR definitief van kracht zal zijn er veel advieswerk verricht zal moeten worden op dit gebied. Klanten zijn zich langzaamaan bewust aan het worden dat er werk aan de winkel is en vallen terug op ons als vertrouwd adviseur door onze gekende focus op informatiebeveiliging.**

**De prestaties van de organisatie op het gebied van informatiebeveiliging zijn goed. Het primaire proces wordt volledig bepaalt en gestuurd door voorwaarden en eisen op het gebied van informatiebeveiliging. Verbeteringen vinden continue en veelal "on-the-fly" plaats.**

**De directie heeft geen trends geconstateerd in afwijkingen nog in corrigerende maatregelen. Het proces van monitoren, meten, auditen gaat in een zeer hoog dagelijks tempo. Het is een praktisch proces waarbij voortdurend gecommuniceerd wordt door belanghebbenden. De doelstelling op het gebied van informatiebeveiliging is primair het veiligstellen van processen van onze klanten; is informatie beschikbaar als het beschikbaar moet zijn, is informatie vertrouwelijk als het vertrouwelijk moet zijn en klopt de informatie als het over integriteit gaat. Hierin presteren we zeer goed; er zijn geen situaties geweest die naar directieniveau geëscaleerd moesten worden**

**De directie ontvangt steeds positieve feedback, het management is primair gefocust op informatiebeveiliging en beschikt over voldoende middelen om de doelstellingen te behalen. Onder het personeel is groot draagvlak voor het informatiebeveiligingsbeleid.**

**Voorgaand jaar was de conclusie dat we wat achter liepen op het gebied van formele risicoanalyse en risico beoordeling. Dat is dit jaar aanzienlijk verbeterd; de organisatie heeft hiertoe goede tools beschikbaar gekregen en deze ook opgepakt voor het produceren van risicoanalyses. Een verbeterpunt dat de directie ziet is het werken met risicoanalyse die meer gebaseerd zijn op scenario's.**

**Al met als heerst er grote tevredenheid over de uitvoering van de in 2014 genomen strategische beslissing om te gaan voor een ISO27001 certificering. We zijn erin geslaagd om niet alleen een papiertje te halen maar om de kwaliteit en professionaliteit van de organisatie op heel veel punten grondig te hebben verbeterd.**

De directeur

Rutger de Nooij

19-9-2017

## Deltacom directiebeoordeling 2018

Eind augustus was het zover, onze eerste 3 jaarlijkse hercertificering voor ISO27001:2013. Een certificaat is na 3 jaar verlopen en dan moet een hercertificering plaats vinden. Daarnaast vonden we het na drie jaar tijd voor een ander bureau dat de externe audits verzorgd en zijn we overgestapt van Lloyds naar DNV-Gl.

Drie dagen lang is de auditor geweest en heeft al onze processen doorgelicht. Het was voor iedereen weer een leuke en leerzame periode waarin er veel gepraat is over hoe we informatiebeveiliging toepassen binnen ons bedrijf en hoe we de normen optimaal voor ons kunnen laten werken. De ISO norm schrijft ons voor wat we moeten regelen en ons managementsysteem laat zien hoe we dat hebben aangepakt en vooral hoe we het proces van voortdurend verbeteren vorm geven. De auditor was enthousiast over de slimme manieren die we de afgelopen tijd gevonden hebben om ons werk beter te doen en nog veiligere omgevingen voor onze klanten te kunnen opzetten. Een goed rapport met alleen maar dikke voldoendes.

Kort daarop was het weer Prinsjesdag, de derde dinsdag van september, het vaste moment bij Deltacom dat we de verplichte “managementreview” beleggen en naar aanleiding waarna de directie haar beoordeling schrijft. Onderwerp van gesprek was natuurlijk de zeer positieve beoordeling door DNV-GL en de geslaagde hercertificering. We stellen vast dat de fase van ad-hoc reageren op problemen en storingen definitief achter ons ligt en dat we een pro-actieve service organisatie zijn met een volwassen niveau van informatiebeveiliging. Als we kijken naar het veel gebruikte model voor de beoordeling van niveaus van informatiebeveiliging, het “security maturity model”(zie schema 1) dan kunnen we concluderen dat de organisatie zich definitief in de “managed/optimised” fase 4/5 bevindt.

| Veiligheidsaspect | 1. INITIEEL | 2. HERHAALBAAR | 3. GEDEFINEERD | 4. BEHEERST | 5. CONTINUE |
|---|---|---|---|---|---|
| *Patchmanagement en antivirus* | Inconsistente, automatische updates, geen rapportage | Enige sprake van automatisering en rapportage | Gedocumenteerd en consistent toegepast | Meetbaar en volledige rapportage afgedwongen door end-point tools | Continue verbetering en innovatie |
| *Firewalls en scheiding van netwerken* | Eenvoudige router met firewall, ad hoc gebruik van software firewalls | Firewall appliance met DMZ | Meerdere firewalls en netwerk segmentatie | Gecentraliseerd beheer van firewalls en configuratiebeheer | Continue verbetering en innovatie |
| *Identiteitsbeheer en toegangscontrole* | Ad hoc zonder onderliggend proces | Domein gebruikers & computers met basale rechtenstructuur | Gedocumenteerd en herhaalbaar proces inclusief een JML proces | Gebruik van tools voor analyse, visualisatie en rapportage | Continue verbetering en innovatie Continue verbetering en innovatie |
| *Beheer van middelen en de inzet ervan* | Niet aanwezig | Middelenlijst beschikbaar | Systeem voor het vinden van middelen en rapportage | Veranderingsbeheer, licentiebeheer | Continue verbetering en innovatie |
| *Informatie classificatie en bescherming* | Niet aanwezig | Ad hoc bestands en/of schijfversleuteling, enige sprake van visuele labels | Gestructureerde data classificatie | Discovery, systemen voor het tegengaan van dataverlies, rechtenbeheer | Continue verbetering en innovatie |
| *Monitoring, alarmering en* | Niet aanwezig | Enige sprake van logging, inconsistente monitoring | Toepassing van basale SIEM, basaal continuïteitsplan | SIEM tools volledig ingezet, periodieke evaluatie, “response & recovery” tests | Continue verbetering en innovatie |
| *Risicomanagement en bestuur* | Niet aanwezig | Ad hoc risico analyse, basaal veiligheidsbeleid | Periodieke risico analyse, risico’s verkleinen, ad hoc bewustzijnstrainingen | Periodieke evaluatie van beleid, training en actieve controle op compliance | Continue verbetering en innovatie |

VOLWASSENHEIDSMODEL INFORMATIEBEVEILIGING

Kijkend naar de algemene beschikbaarheid van onze diensten dan zien we dat er steeds minder incidenten van de categorie “beschikbaarheid”, vastgelegd worden in ons ticketingsysteem en dat als er incidenten zijn deze een kleinere impact hebben dan voorheen; onze klanten dus hebben kunnen genieten van een hoger niveau van beschikbaarheid.

Kansen voor continue en voortdurende verbetering zijn er ook. Het verder implementeren van regelmatige penetratie testen door ethische hackers en “red teaming” oefeningen waarbij de weerbaarheid van de organisatie tegen (cyber)incidenten wordt vergroot wordt staan op de planning.

# Deltacom directiebeoordeling 2019

Hoe zit het met ons managementsysteem voor informatiebeveiliging, het ISMS? Werkt het goed en is het geschikt, adequaat en doeltreffend? Deze vragen moeten we ons als organisatie natuurlijk voortdurend stellen maar op de derde dinsdag van september (Prinsjesdag) in het bijzonder. Onze ISO27001:2013 certificering schrijft dit immers voor en daarom beleggen we ieder jaar op de derde dinsdag van september onze “managementreview” en rapporteert ons management officieel aan de directie. Voor een relatief kleine organisatie als Deltacom is dat altijd wel een apart moment omdat management en directie dagelijks overlegt, rapporteert en wederzijds feedback geeft. Maar even een rustmoment kiezen en uit de cirkel stappen kan geen kwaad en geeft gelegenheid zaken even op een rijtje te zetten.

Mooie vooruitgang boekten we op het gebied van de beveiliging. Na een lange zoektocht naar een geschikte partner voor pentesten hebben we eindelijk een partner gevonden die het gezochte niveau aankan en met concrete aanbevelingen kon komen na afloop van de tests. De beveiliging werd beoordeeld als “goed” en de aanbevelingen konden binnen een maand gerealiseerd worden.

Wijzigingen in externe en interne onderwerpen die invloed hebben op ons managementsysteem hebben plaats gevonden:

- Intern hebben we een medewerker nu eindverantwoordelijk gemaakt voor het ISMS;
- We overwegen volgend jaar te gaan voor een ISAE3402 type I en type II certificering, dit zal van invloed zijn op de huidige inrichting van het ISMS;
- We implementeren in 2019/20 een nieuw helpdesksysteem dat meer efficiency gaat brengen in de stroom tickets.

Kijkend naar de algemene beschikbaarheid van onze diensten dan zien we dat er weer minder incidenten van de categorie “beschikbaarheid”, zijn geregistreerd en dat deze een kleinere impact hebben dan voorheen; onze klanten hebben dus kunnen genieten van een hoger niveau van beschikbaarheid. De resultaten van monitoring, geautomatiseerde logging en geautomatiseerde auditing, kortom het meten zijn goed en worden op duidelijke en begrijpelijke wijze gepresenteerd aan medewerkers. Auditresultaten worden momenteel direct “on-the-fly” behandeld; hier gaan we de komende periode meer structuur in brengen.

Een belangrijk incident was de uitval van het datacenter op 30 april. Gelukkig heeft dit geen ernstige impact gehad op onze dienstverlening om dat dit in de nacht van zaterdag op zondag gebeurde op Koninginnedag. Deze gebeurtenis is geëvalueerd en we zijn tot de conclusie gekomen dat ons continuïteitsplan verbeterd kon worden. Op dit moment zijn we bezig met optimalisaties die eind dit jaar afgerond moeten zijn.

Besluiten:

- Dit jaar moeten alle verbeteringen rond continuïteit doorgevoerd zijn;
- het interne auditing proces moet dit jaar volledig geoptimaliseerd zijn.

De directie

19-9-2019

Rutger de Nooij