DATACLASSIFICATIE BIJ CLOUDOMGEVINGEN

Ron Velthoen CISA
11 oktober 2018

Agenda

- Aanpak classificatie
- ISO27K
- ISAE3402
- ISAE3000
- SOC 1,2,3

Aanpak data classificatie in cloud omgeving

- Onderscheid cloud infrastructuur Versus "Instellingsapplicatie"
- Beveiliging cloud provider
- Aanvullende maatregelen door instelling

Certificeringen, audits

- Onderscheid certificering en audit
- ISO27001: ISMS
- Relatie ISO27002
- Voorbeelden audits:

  →ISAE3000

  →ISAE3402

  →SOC 1/2/3

Onderscheid certificering, type 1 en 2

Opzet: beleid

Bestaan: vertaling naar taken, bevoegdheden, processen en procedures

Werking: toetsing of processen en procedures volgens beleid worden uitgevoerd

- Certificering: alleen opzet en bestaan
- Type 1: alleen opzet en bestaan
- Type 2: opzet, bestaan en werking
- **Werking** geeft meer inzicht en betrouwbaarheid

ISO27K

- ISO27001: **ISMS**, Information Security Management System
- ISO27002: best practices, **geen** certificering mogelijk
- ISO27017: cloud diensten, Certificering **alleen** icm ISO27001
- ISO27018: privacy in de cloud, Certificering **alleen** icm ISO27001

Wat houdt een ISO27001 certificering in?

- **Audit**: uitgevoerd door een onafhankelijk en gecertificeerd auditor
- **Na akkoord auditor**: certificaat door een certificerende instelling
- **Certificerende instelling**: Raad van Accreditatie (www.rva.nl)
- **Geldigheidstermijn certific**aat: 3 jaar
- **Jaarlijks**: audit
- **Certificaten controleren**: website van de certificerende instelling
- **Alleen opzet en bestaan (geen werking)**

Hoe een ISO27001 certificaat te beoordelen?

- Opvragen certificaat
- Opvragen Verklaring van Toepasselijkheid (Statement of Applicability)
- Beoordelen aansluiting scope certificaat vs clouddienst
- Beoordelen maatregelen Verklaring van toepasselijkheid (pas toe of leg uit/comply or explain)
- Beoordelen onderbouwing van niet uitgevoerde maatregelen

ISAE3402

- **Vertrouwelijk** type 1 (opzet en bestaan) of 2 (opzet, bestaan en werking)
- **Vaste vorm**, kijkt terug in de tijd bv jaar
- **Non Disclosure Verklaring** (NDA)
- **Primair** voor accountant van klanten
- **Normenkader** beperkte set maatregelen
- **Soms**: uitgebreide set -> meer waarde
- **Beoordeling:** gecertificeerd auditor

ISAE3000

- **Vertrouwelijk**, type 1 of 2
- **Non Disclosure Verklaring** (NDA)
- **Vormvrij**, kijkt terug in de tijd bv jaar
- **Normenset:** auditor
- **Beoordeling:** gecertificeerd auditor

SOC 1,2,3 type 1 of 2

- **SOC1**: Voor accountant klant, beperkte waarde
- **SOC2**: gericht op **beveiliging, meest waardevol**
- **SOC3**: "zegel” op website **beperkte waarde**
- **NDA**
- **Uitgebreide maatregelen set**
- **Beoordeling:** gecertificeerd auditor

Maatregelen door instellingen

- **Instellingen**: ook zelf diverse beveiligingsmaatregelen
- Voorbeelden :

  →Logische toegangsbeveiliging applicatie

  →Encryptie

  →Applicatie backup

  →Etc.

Vragen

Ron Velthoen

E-mail: ron.velthoen@surfmarket.nl

www.surf.nl

Social media:

Samen aanjagen van vernieuwing

Deze presentatie valt onder een Creative Commons Naamsvermelding 4.0 Internationaal-licentie.

SURF hanteert bij voorkeur de licentie Creative Commons Naamsvermelding 4.0 Internationaal.
Deze licentie is van toepassing op alle informatie in deze presentatie, met een aantal uitzonderingen:

- Voor informatie op websites waarnaar wordt verwezen, kunnen andere licenties en voorwaarden gelden.
- De volgende rechten worden door Creative Commons-licentie niet gewijzigd en blijven dus van kracht:
  1. Octrooirechten en merkrechten
  2. De rechten van anderen, ofwel op onderdelen van deze website ofwel op de wijze waarop de website wordt gebruikt, zoals het portretrecht of privacyrecht

Samen aanjagen van vernieuwing