# "Baselines: eigenwijsheid of wijsheid?"

Een afrondende 'beschouwende' presentatie

Ing. Ernst J. Oud CISA CISSP

**kineta ICT advies**

Ing. Ernst J. Oud CISSP CISA

Nijenbeekseweg 16
7383 BD Voorst

Telefoon 06 - 239 69 309
www.kineta.nl
info@kineta.nl

Philips
Toshiba

Crypsys Data Security
Getronics Business Continuity (a.k.a. CUC)
Urenco
Deloitte ERS
Microsoft

Kineta ICT advies

- Consultancy IB / BCM > 20 projecten
- ISO27001 Lead Auditor – BSI > 60 relaties, > 300 auditdagen
- Docent > 65 dagen

kineta



# Notities tijdens de sessie

- …

kineta

# ISO27001 / ISO27002

Sinds 2005 toonaangevend

> 50.000 organisaties gecertificeerd
> 1.000 in NL

Managementsysteem (PDCA)
Annex A. : 114 maatregelen

En… is geen baseline !!!

kineta



ISO/IEC – JTC1 – SC27 - NEN

> 3.000 professionals wereldwijd

ISO normen worden gratis (?) voor u onderhouden !

Kunt u het zelf beter?

kineta

# Waarneming:
# Levenscyclus van een baseline

- Er is ergens een idee dat de IB beter moet
- Een groep(je) enthousiastelingen gaat aan de slag
  - Men inventariseert niet voldoende wat er al is
  - Men vergeet dat implementatie het moeilijkst is (wel “wat” maar geen “hoe”)
- Door de eigenwijsheid komt er een heftige “baseline”
- Het werkveld schrikt ervan, “dit is niet te implementeren”
- Er gebeurt heel lang (vaak jaren!) niets/weinig
- Terug naar “af”…

kineta



# Interprovinciale
# Baseline Informatieveiligheid

| | | | |
|---|---|---|---|
| 1790 | maatregelen | baseline | 94% |
| 117 | maatregelen | > baseline | 6% |
| 1907 | maatregelen totaal | | |

**B 1** *Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.*

- 1 Voorafgaand aan vernietiging moet commercieel gevoelig afval duidelijk worden geïdentificeerd en gescheiden van ander afval worden bewaard.
- 2 Personeel dat niet geautoriseerd is voor toegang tot vertrouwelijk materiaal dient ook geen toegang te hebben tot afval gemerkt met hetzelfde vertrouwelijkheidsniveau.
- 3 Versnipperen dient ervoor te zorgen dat afval niet kan worden gereconstrueerd.
- 4 De inhoud van magnetische gegevensdragers moet worden overschreven voorafgaand aan afstoting.
- 5 Optische schijven die vertrouwelijke informatie bevatten moeten voorafgaand aan afstoting worden gebroken.
- 6 Niet-vluchtig geheugen moet worden overschreven of vernietigd voorafgaand aan afstoting.
- 7 Wanneer gegevens overschreven zijn dienen er controles uitgevoerd te worden om er zeker van te zijn dat de procedure waarmee de gegevens overschreven zijn goed heeft gewerkt.
- 8 Verscheur documenten die kunnen worden weggegooid.
- 9 Versnipper afval.
- 10 Maak pulp van het afval.
- 11 Laat afval ontbinden.
- 12 Vermaal afval.
- 13 Verbrand afval.
- 14 Gebruik zuur of chemische technieken.
- 15 Herformatteer afval.
- 16 Demagnetiseer afval.
- 17 Als de gegevens van herbruikbare gegevensdragers niet langer nodig zijn, dienen ze te worden verwijderd.

kineta

# Maximale inhoud baseline

- Beleid – Maatregelen – Review
- Maatregelen:
  - Beschikbaarheid — backup, reserve hw/sw, hang- en sluitwerk
  - Integriteit — anti-malware, awareness, monitoring
  - Vertrouwelijkheid — wachtwoord, firewall, encryptie
- Pragmatische tooling voor baseline+

kincta



# Wat kan er beter

- Realisatie dat van implementeren de IB beter wordt
- Maak dus vooral concrete praktijkrichtlijnen
- Luister naar het werkveld
- Ambitie en realiteitszin bijstellen
- Zorg voor tooling, ondersteuning, fora, …
- Regel onderhoud
- Zorg voor budget voor implementatie
- En: zorg dat de baseline ook de PDCA cyclus bevat!

kincta

# ISO27001 (ISMS)

4.1 Inzicht verkrijgen in de organisatie en haar context
4.2 Inzicht verkrijgen in de behoeften en verwachtingen van belanghebbenden
4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen
4.4 Managementsysteem voor informatiebeveiliging
5.1 Leiderschap en betrokkenheid
5.2 Beleid
5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie
6.1 Maatregelen om risico's te beperken en kansen te benutten
6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken
7.1 Middelen
7.2 Competentie
7.3 Bewustzijn
7.4 Communicatie
7.5 Gedocumenteerde informatie
8.1 Operationele planning en beheersing
8.2 Risicobeoordeling van informatiebeveiliging
8.3 Informatiebeveiligingsrisico's behandelen
9.1 Monitoren, meten, analyseren en evalueren
9.2 Interne audit
9.3 Directiebeoordeling
10.1 Afwijkingen en corrigerende maatregelen
10.2 Continue verbetering



# ISO27001 (ISMS – baseline)

4.1 Inzicht verkrijgen in de organisatie en haar context
4.2 Inzicht verkrijgen in de behoeften en verwachtingen van belanghebbenden
4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen
4.4 Managementsysteem voor informatiebeveiliging
5.1 Leiderschap en betrokkenheid
5.2 Beleid
5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie
6.1 Maatregelen om risico's te beperken en kansen te benutten
6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken
7.1 Middelen
7.2 Competentie
7.3 Bewustzijn
7.4 Communicatie
7.5 Gedocumenteerde informatie
8.1 Operationele planning en beheersing
8.2 Risicobeoordeling van informatiebeveiliging
8.3 Informatiebeveiligingsrisico's behandelen
9.1 Monitoren, meten, analyseren en evalueren
9.2 Interne audit
9.3 Directiebeoordeling
10.1 Afwijkingen en corrigerende maatregelen
10.2 Continue verbetering

# ISO27001 (Annex A.)

A.5.1 Management direction for information security
A.6.1 Internal organization
A.6.2 Mobile devices and teleworking
A.7.1 Prior to employment
A.7.2 During employment
A.7.3 Termination and change of employment
A.8.1 Responsibility for assets
A.8.2 Information classification
A.8.3 Media handling
A.9.1 Business requirements of access control
A.9.2 User access management
A.9.3 User responsibilities
A.9.4 System and application access control
A.10.1 Cryptographic controls
A.11.1 Secure areas
A.11.2 Equipment
A.12.1 Operational procedures and responsibilities
A.12.2 Protection from malware
A.12.3 Backup
A.12.4 Logging and monitoring
A.12.5 Control of operational software
A.12.6 Technical vulnerability management
A.12.7 Information systems audit considerations
A.13.1 Network security management
A.13.2 Information transfer
A.14.1 Security requirements of information systems
A.14.2 Security in development and support processes
A.14.3 Test data
A.15.1 Information security in supplier relationships
A.15.2 Supplier service delivery management
A.16.1 Management of information security incidents and improvements
A.17.1 Information security continuity
A.17.2 Redundancies
A.18.1 Compliance with legal and contractual requirements
A.18.2 Information security reviews



# ISO27001 (Annex A. – baseline)

A.5.1 Management direction for information security
A.6.2 Mobile devices and teleworking
A.7.2 During employment
A.8.3 Media handling

A.9.1 Business requirements of access control
A.9.2 User access management
A.11.1 Secure areas
A.12.2 Protection from malware

A.12.3 Backup
A.12.4 Logging and monitoring
A.12.6 Technical vulnerability management
A.14.1 Security requirements of information systems
A.16.1 Management of information security incidents and improvements
A.18.1 Compliance with legal and contractual requirements

# Baseline?

ISO27002:2013

*Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations.*

ISO27002:2005

data protection and privacy of personal information
protection of organizational records
intellectual property rights

information security policy document
allocation of information security responsibilities
information security awareness, education, and training
correct processing in applications
technical vulnerability management
business continuity management
management of information security incidents and improvements

kineta



kineta

Knowledge speaks, but wisdom listens.

Jimi Hendrix