Security Awareness Sessie FITZME, tbv de coaches

21 mei 2019

Bart van der Kallen, CISM, CIPP/E

ZILVERBLAD
informatiebeveiliging

AGENDA

- Wie ik ben
- Aanleiding voor deze sessie
- De norm: NEN 7510 / ISO 27001
- De (invulling van de) komende audits
- Fitzme omgeving met Fitzme IB-beleid
- Aandachtspunten voor alle medewerkers
- Vragen / opmerkingen?

Aanleiding voor deze sessie

- Fitzme wil NEN 7510 / ISO 27001-certificering, daarmee ‘bewijs’ dat InformatieBeveiliging (IB) op orde is
- De medewerker is cruciaal voor een ‘veilige’ bedrijfsvoering
- Security awareness is daarom een verplicht onderdeel
- Vanwege ‘aantoonbaarheid’ een aanwezigheidsregistratieformulier *

AGENDA

- Wie ik ben
- Aanleiding voor deze sessie
- **De norm: NEN 7510 / ISO 27001**
- De (invulling van de) komende audits
- Fitzme omgeving met Fitzme IB-beleid
- Aandachtspunten voor alle medewerkers
- Vragen / opmerkingen?

NEN 7510 (≈ ISO 27001)

Via een continu systeem van monitoren en verbeteren

de bescherming van **B**eschikbaarheid, **I**ntegriteit & **V**ertrouwelijkheid van alle bedrijfsinformatie managen,

en vervolgens door een onafhankelijke instantie laten vaststellen dat dit op orde is,

zodat dmv een certificering aangetoond kan worden dat de organisatie ‘in control’ is (business waarde!)

NEN 7510 zorgt voor aantoonbaarheid

- NEN 7510 is ‘n ISMS (Information Security Mngt Syst)
- Met ‘n normenkader met 14 onderdelen (114 aspecten)
- Die aandacht moeten krijgen (!)
- Op basis waarvan certificering mogelijk is
- Door een onafhankelijke externe instantie
- Op basis van objectief bewijs
- Op opzet, bestaan en werking

Niet alles hoeft ingevuld / opgelost te zijn, het accent in een audit ligt niet op de Maatregelen zelf, maar op de werking van het managementsysteem!

NEN 7510 / NEN 7512 / NEN 7513

NEN 7510 is de norm voor het organisatorisch en technisch inrichten van de informatiebeveiliging in de zorg

NEN 7512 is een nadere invulling van NEN 7510 m.b.t. veiligheid van gegevensuitwisseling tussen partijen in de zorg

NEN 7513 is een nadere invulling van NEN 7510 m.b.t. het vastleggen van acties op elektronische cliëntdossiers: de logging (= vereiste vanuit AVG)

NEN 7510 kent 14 domeinen (1)

	Toelichting
5. Informatiebeveiligingsbeleid	5
6. Organiseren van informatiebeveiliging	6
7. Veilig personeel	7
8. Beheer van bedrijfsmiddelen	8
9. Toegangsbeveiliging	9
10. Cryptografie	10
11. Fysieke beveiliging en beveiliging omgeving	11

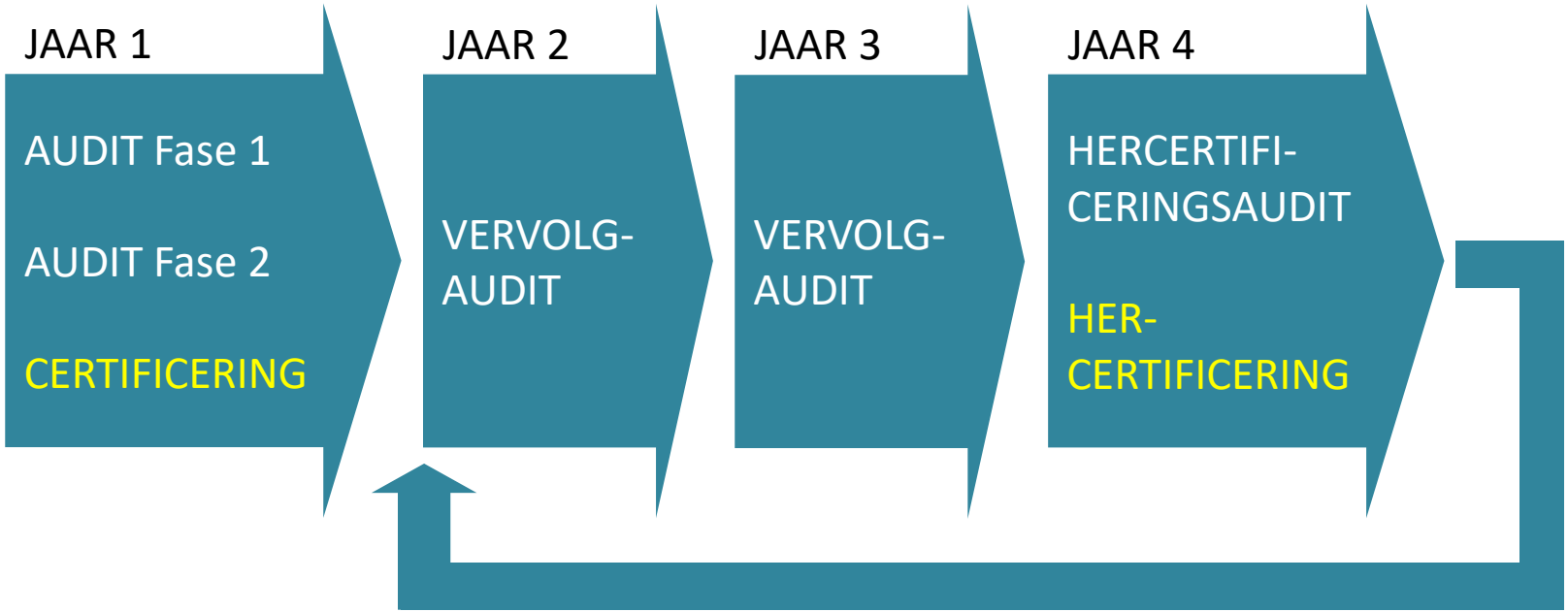
NEN 7510 kent 14 domeinen (2)

	Toelichting
12. Beveiliging bedrijfsvoering	12
13. Communicatiebeveiliging	13
14. Acquisitie, ontw. en onderh. van inform.syst.	14
15. Leveranciersrelaties	15
16. Beheer van beveiligingsincidenten	16
17. Bedrijfscontinuïteitsbeheer	17
18. Naleving	18

AGENDA

- Wie ik ben
- Aanleiding voor deze sessie
- De norm: NEN 7510 / ISO 27001
- **De (invulling van de) komende audits**
- Fitzme omgeving met Fitzme IB-beleid
- Aandachtspunten voor alle medewerkers
- Vragen / opmerkingen?

Het auditprogramma



De audits

<u>Fase 1 audit:</u>

- 1 dag
- Toetsing op opzet ISMS, (verplichte) documentatie, support door Directie

<u>Fase 2 audit:</u>

- 2 dagen
- Interviews mbt relevante norm-hoofdstukken
- Meestal ‘rondje lopen’ (nav H11: fysieke beveiliging)

Voorbije & komende acties Fitzme

Verplichte documentatie opzetten, beleid vaststellen en uitdragen, risico's inventariseren, maatregelen kiezen en implementeren, de PDCA-cyclus aantoonbaar toepassen, controle acties uitvoeren, …

AUDIT FASE 1 → 01-07-2019

Wat 'aandachtspunten' wegwerken, interviews voorbereiden, …

AUDIT FASE 2 → 16- + 17-09-2019

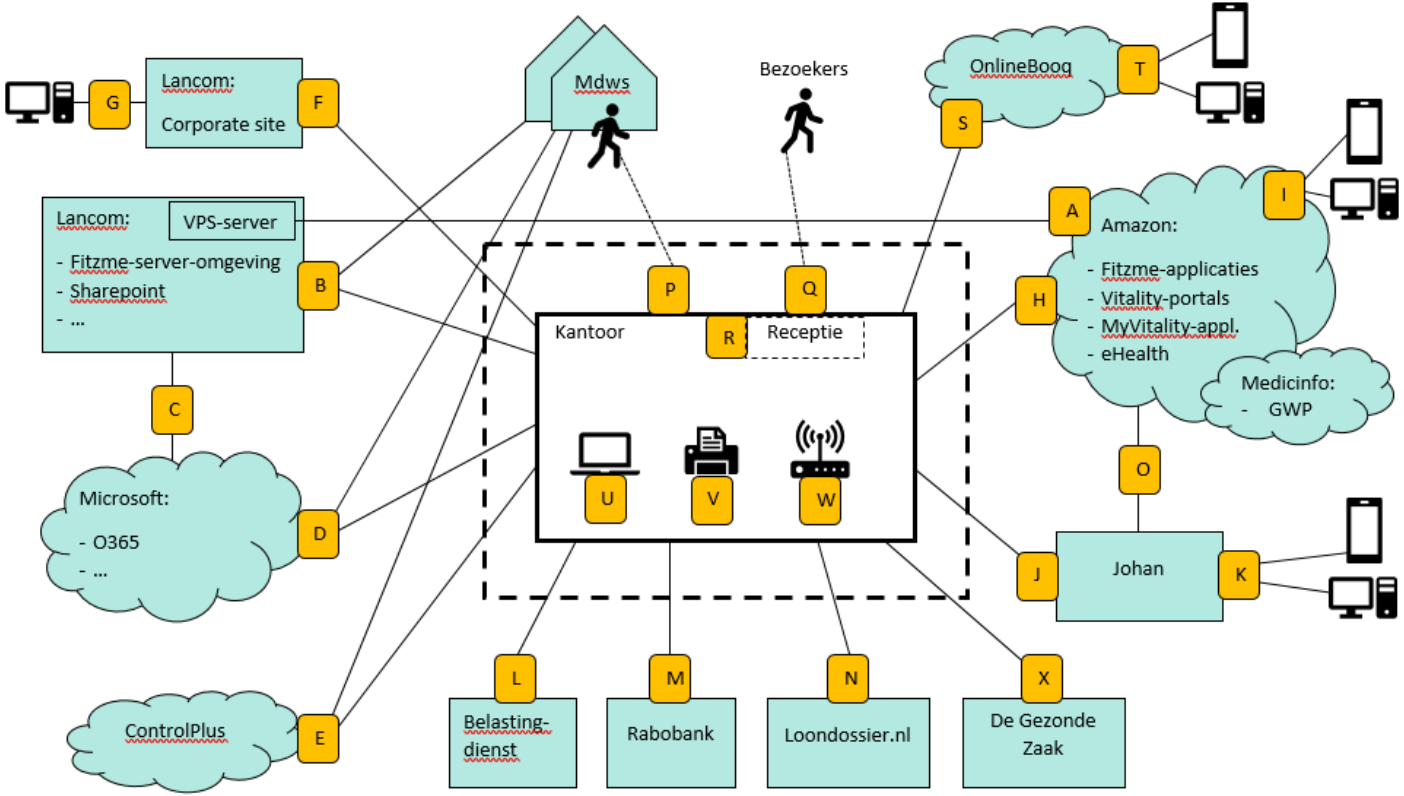
Evt 'tekortkomingen' wegwerken

CERTIFICERING → ??? (≈ eind oktober)

AGENDA

- Wie ik ben
- Aanleiding voor deze sessie
- De norm: NEN 7510 / ISO 27001
- De (invulling van de) komende audits
- **Fitzme omgeving met Fitzme IB-beleid**
- Aandachtspunten voor alle medewerkers
- Vragen / opmerkingen?

De te certificeren omgeving



Belangrijke IB-documenten

<u>Via Sharepoint vind je altijd de laatste versie van:</u>

FIT-IBB fitzme informatiebeveiligingsbeleid
FIT-IBB-BPD beleid per deelgebied
Verzoek: lees en signaleer 'afwijkingen'

Fitzme Geheimhoudingsverklaring
Fitzme Gedragscode computerfaciliteiten
Fitzme BYOD reglement

AGENDA

- Wie ik ben
- Aanleiding voor deze sessie
- De norm: NEN 7510 / ISO 27001
- De (invulling van de) komende audits
- Fitzme omgeving met Fitzme IB-beleid
- **Aandachtspunten voor alle medewerkers**
- Vragen / opmerkingen?

Aandachtspunten voor alle medewerkers

- Ben altijd scherp op IB en Privacy, maar op de auditdagen nog een beetje scherper…
- Clear screen en clear desk
- Toegang tot bedrijfsruimtes
- Geen documenten bij de printer
- Geen geeltjes met wachtwoorden
- Etc

De totale kwaliteit van IB wordt bepaald door hoe veel medewerkers omgaan met heel veel kleine aspecten!

Vragen / opmerkingen?

Navolgende slides bevatten een nadere specificatie per hoofdstuk van de nen7510

Toelichting Hoofdstuk 5

1. Directieaansturing van en –steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving

Bijvoorbeeld:

- Welke beveiligingsdoelen?
- Hoe gaan we ons doel bereiken?
- Wat is het mandaat van de organisatie?

terug

Toelichting Hoofdstuk 6

1. Interne organisatie
2. Mobiele apparatuur en telewerken

Bijvoorbeeld:

- Wie coördineert de informatiebeveiliging?
- Hoe lopen communicatie- en rapportagelijnen?
- Scheiding van taken
- Beleid voor mobiele apparatuur

terug

Toelichting Hoofdstuk 7

1. Voorafgaand aan het dienstverband
2. Tijdens het dienstverband
3. Beëindiging en wijziging van dienstverband

Bijvoorbeeld:

- Screening tijdens sollicitatie
- Geheimhoudingsverklaringen
- Opleiden, bijscholen, bewust maken
- Disciplinaire maatregelen

terug

Toelichting Hoofdstuk 8

1. Verantwoordelijkheid voor bedrijfsmiddelen
2. Informatieclassificatie
3. Behandelen van media

Bijvoorbeeld:

- Classificeren en labelen van middelen
- Overzicht en beheer op middelen
- Verwijderbare media adequaat beheren en afvoeren
- Richtlijnen voor gebruik

terug

Toelichting Hoofdstuk 9

1. Bedrijfseisen voor toegangsbeveiliging
2. Beheer van toegangsrechten van gebruikers
3. Gebruikersverantwoordelijkheden
4. Toegangsbeveiliging van systeem en toepassing

Bijvoorbeeld:

- Gebruikersregistratie, -identificatie, -authenticatie
- Welke rol/functie mag welke autorisatie(s)?
- Systeem voor wachtwoordbeheer

terug

Toelichting Hoofdstuk 10

1. Cryptografische beheersmaatregelen

Bijvoorbeeld:

- Beleid tav versleuteling van gegevens
- Beheer van de cryptografische sleutels

terug

Toelichting Hoofdstuk 11

1. Beveiligde gebieden
2. Apparatuur

Bijvoorbeeld:

- Fysieke toegangsbeveiliging
- Stroomvoorziening
- Beveiliging van bekabeling

terug

Toelichting Hoofdstuk 12

1. Bedieningsprocedures en verantw.heden
2. Bescherming tegen malware
3. Back-up
4. Verslaglegging en monitoren
5. Beheersing van operationele software
6. Beheer van technische kwetsbaarheden
7. Overwegingen betreffende audits van informatiesystemen

Bijvoorbeeld: functiescheiding, change mngt, …

terug

Toelichting Hoofdstuk 13

1. Beheer van netwerkbeveiliging
2. Informatietransport

Bijvoorbeeld:

- Scheiding in netwerken
- Overeenkomsten over informatietransport
- Elektronische berichten

terug

Toelichting Hoofdstuk 14

1. Beveiligingseisen voor informatiesystemen
2. Beveiliging in ontwikkel- en ondersteuningsprocessen
3. Testgegevens

Bijvoorbeeld:

- Mobiele applicaties
- Cloud computing
- Open source
- Beleid voor systeemtesten

terug

Toelichting Hoofdstuk 15

1. Informatiebeveiliging in leveranciersrelaties
2. Beheer van dienstverlening van leveranciers

Bijvoorbeeld:

- Beveiligingsaspecten in overeenkomsten
- Beveiliging van netwerkdiensten
- Beheer van dienstverlening

terug

Toelichting Hoofdstuk 16

1. Beheer van informatiebeveiligingsincidenten en -verbeteringen

Bijvoorbeeld:

- Het melden van incidenten
- Rapporteren van zwakke plekken in de IB
- Respons op informatiebeveiligingsincidenten
- Verzamelen van bewijsmateriaal

terug

Toelichting Hoofdstuk 17

1. Informatiebeveiligingscontinuïteit
2. Redundante componenten

Bijvoorbeeld:

- Maximale Uitvalsduur (MUD) per dienst / toepassing
  (= RTO = Recovery Time Objective)
- Maximaal Gegevensverlies (MGV) per dienst / toepassing
  (= RPO = Recovery Point Objective)
- Concrete (uitwijk)plannen of strategie
- Periodiek testen en bijwerken van plannen

terug

Toelichting Hoofdstuk 18

1. Naleving van wettelijke en contractuele eisen
2. Informatiebeveiligingsbeoordelingen

Bijvoorbeeld:

- Voer interne audits uit
- Per proces wet- en regelgeving in acht nemen
- Archiveringstermijnen
- Bewijslast bij overtredingen

terug