**BIO Workshop**20-3-2024  
  
  
**1. Achtergrond**Vanaf 1 januari 2019  
BIO is er om de veiligheid te vergroten  
  
Hoe moet je maatregelingen nemen om de in kaart gebrachte risico’s te mitigeren  
  
Vraagstuk: hoe kan je het normenkader specifiek maken voor jouw organisatie? Door de normen te concretiseren tot concrete maatregelen  
  
ICT bedrijven   
  
Het is bijna een verplichting om als IT leverancier ISO 27001 gecertificeerd te zijn  
  
Jan: bij marktverkenning met de leveranciers neem je al informatiebeveiligingsvraagstukken mee  
Dit biedt veel voordelen voor jou als aanbestedende partij  
  
BIO 2.0: hoe gaan we om met de NIS2   
  
NIS2: Van toepassing op meerdere sectoren, decentrale overheden. Zorgplicht en een meldplicht beveiligingsincidenten  
  
  
Inzage in bedreigen: welke bedreigingen, intern en extern, zijn er en wat moeten we hiermee?  
  
Virbir: hebben we informatie in huis waarvan kennisname door niet-geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, bondgenoten (denk bijv. aan NAVO) of van 1 of meerdere ministeries.  
  
🡪 Departementaal Vertrouwelijk is het niveau waar wij binnen de Belastingdienst mee werken  
 **Slide:** Nog een voorbeeld VIRBI Verzending gerubriceerde informatie.  
Hoe doe je dit, op welke manier etc. etc.  
  
**2. Opzet BIO**  
Totaal 114 Controls  
  
Onze controlelijst:  
• Fysieke beveiliging: verwachten dat dit geregeld is. Hier toetsen wij niet op.  
• Netwerkbeveiliging: hierbij verwachten we dat het aan de voorkant, wat er binnenkomt, vanuit IV geregeld is. Specifiek: het netwerk van de Belastingdienst, technische beveiligingsinrichting IV. Bijvoorbeeld inrichting SIEM en SOP. Dus vanuit onze MDT rol gaan we hier niet de nodige vragen over stellen.  
  
We toetsen het menselijk handelen, behalve het inrichten van systemen, de autorisatiematrix, hoe het logisch toegangsbeheer geregeld.   
Het is aan een teammanager om op basis van die richtlijnen de mensen toegang te verlenen.  
We hebben de IMS rollen.  
Wij toetsen de functionaliteiten van een applicatie, wat doen ze met de applicatie.

**Opzet BIO: vanuit CSO healthcheck Belastingdienst** een eerste scan te doen hoe het ervoor staat qua informatiebeveiliging   
**INTERESSANTE SLIDE:** Dit is een snapshot. Eigenlijk kun je je daar op focussen.  
Hoe organiseer ik informatiebeveiliging binnen onze directie?  
bio-overheid.nl/bio-practices  
  
BIO-18: hier kom je uit bij de directie. Op welke manier is de navolging geregeld wat betreft procedures **3. Basisbeveiligingsniveaus**Wat moet je doen om jou niveau vast te stellen,  
maar ook je BIV niveau  
  
Hier wordt je beschikbaarheid, integriteit, betrouwbaarheid bepaald  
  
Bij Belastingdienst is afgesproken dat niks boven BBN2 uitkomt.  
De Belastingdienst hanteert BBN2: alles wat je hebt aan informatiesystemen  
Als je niks toetst dan is BBN2 de standaard  
**Notitie:** Het vertrouwelijkheidsniveau is leidend voor  
  
Vertrouwelijkheid is leidend. Als het midden is, dan is het altijd BBN2.  
**Notitie:** Je rekent van BIV naar BBN.  
**Notitie:** BBN3 is bedoelt voor statelijke actoren  
  
De integriteit: voor Belastingdienst belangrijk, je moet kunnen verantwoorden waarom je gaat innen en heffen  
  
**Vertrouwelijkheid:** Cybersecurity valt hier ook onder, hoe is het geregeld met jouw systemen.  
Welke maatregelen heb je genomen bij de netwerken van je systemen  
  
  
Vraag: toegang tot bepaalde systemen:  
is het noodzakelijk dat wij kunnen checken dat degene die echt toegang moet hebben dat…  
  
De 6 kritische applicaties: wie hebben allemaal toegang wie zijn dat dan en hoe moet dat?  
Controlelijst gaat zover dat er een autorisatiematrix is.  
Jan: tenzij ze zelf aankomen zetten we hebben nog een paar mensen die nog toegang moeten hebben en wel hierom. Misschien dat ze dan nog verder kunnen toelichten  
Raymond: het is een nuchtere vaststelling. Worden autorisaties beheerd, wie is er verantwoordelijk voor?  
In de vraagstelling uit de controlelijst zit je op een bepaald niveau.  
  
  
**Bevinding constatering:** Als er voor een systeem geen autorisatiematrix is dan is het een constatering dat je totaal geen inzicht hebt wie waar toegang voor heeft.

**Processtappen informatiebeveiliging volgens BIO**Gebruik van de quickscan informatiebeveiliging.  
Handig hulpmiddel  
  
  
**Informatiebeveiliging is riscomanagement**• Bij informatiebeveiliging staat risicobeheersing centraal  
  
**Resultaat risicoanalyse: de heatmap**Kans x Impact  
Bij een heatmap kun je met pijlen aangeven waar je zit en waar je naartoe wil. Dit kun je doen aan de hand van maatregelen  
  
Risico’s ga je:  
• Vermijden  
• Verminderen  
• Overdragen/verzekeren  
• Accepteren  
  
  
**TBB:** Te beschermen belangen

27-3-2024  
  
**Referentiearchitectuur**  
Praktijkvragen op de vraagstelling van de controlelijst  
Hier staan artikelen bij uit de AVG/BIO/AW  
  
Raymond: bij veel processen wordt verwezen naar de general IT controls van de Belastingdienst (die van IV)  
Jan: 9/10 systemen doen alleen iets voor in de cloud  
Geef alvast mee aan leveranciers/marktverkenningen die je doet  
  
Raymond:  
Hoe moeten we het spiegelen aan bewijs

**Authenticatie** bevestigt de gebruikers wie ze zijn  
**Autorisatie** geeft gebruikers toegang tot een informatiebron