



# Quickscan ‘Security Awareness in uw organisatie’

Directie Regie NCTb

*Beveiligingsbewustzijn bij het personeel – internationaal bekend als security awareness – kan bijdragen aan het voorkomen van terrorisme, het terugdringen van criminaliteit en het vroegtijdig signaleren van ongewenst gedrag .*

*Met deze quick scan kunt u alleen of samen met collega’s snel een eerste indruk krijgen van de mate waarin security awareness bij de medewerkers in uw organisatie is ontwikkeld.*

*Heeft uw organisatie een security awareness programma en voldoet dat? En is zo’n programma er nog niet, loopt u dan geen onnodig risico? De quick scan laat u en uw collega’s zien waar verbetering mogelijk is. Doe er uw voordeel mee!*

## Stap 1: Vul de vragen in

Met deze quick scan krijgt u een eerste indruk van de effectiviteit van het security awareness programma in uw organisatie. Security awareness is de mate waarin iedere medewerker op elk niveau in de organisatie het belang en de mate van beveiliging begrijpt, zijn eigen individuele beveiligingsverantwoordelijkheden inziet en daar ook naar handelt. Een organisatie kan er aan de hand van een aantal kritische succesfactoren voor zorgen dat medewerkers ‘security aware’ worden én blijven. Beantwoord eerst de twee vragen die horen bij de verschillende succesfactoren.

### Commitment: (de organisatie moet achter het belang van security awareness staan)

1. Leidinggevend in onze organisatie geven het goede voorbeeld door bijvoorbeeld zelf zichtbaar hun bedrijfsjas te dragen en anderen aan te spreken op het naleven van beveiligingsmaatregelen.

eens      oneens  
5 4 3 2 1

2. De organisatie stelt tijd en geld beschikbaar voor het volgen van security awareness trainingen.

eens      oneens  
5 4 3 2 1

### Cultuur: (security awareness moet onderdeel van de organisatiecultuur zijn)

3. Security awareness en beveiligingsincidenten zijn een vast onderwerp van gesprek binnen onze organisatie.

eens      oneens  
5 4 3 2 1

4. De leidinggevend in onze organisatie stimuleren het personeel om beveiligingsincidenten te melden.

eens      oneens  
5 4 3 2 1

### Communicatie: (regelmatige communicatie over security awareness is belangrijk)

5. Onze communicatie over security awareness is afgestemd op de werkzaamheden die onze organisatie uitvoert.

eens      oneens  
5 4 3 2 1

6. Onze organisatie zet verschillende communicatiemiddelen in (papier, intranet, posters, etc.) om security awareness blijvend onder de aandacht te brengen.

eens      oneens  
5 4 3 2 1

### Coöperatie: (security awareness kun je niet alleen)

7. Ons security awareness programma is opgesteld in samenwerking met de organisaties waarmee wij bij de uitvoering van onze werkzaamheden in aanraking komen, zoals leveranciers, afnemers en onderaannemers.

eens      oneens  
5 4 3 2 1

8. Als er nieuwe beveiligingsmaatregelen zijn, zorgt de verantwoordelijke beveiligingsprofessional binnen onze organisatie er samen met de afdelingen voor dat deze maatregelen worden uitgewerkt en uitgerold.

eens      oneens  
5 4 3 2 1

### Bewustzijn: (security awareness dient een tweede natuur te zijn)

9. Binnen onze organisatie delen we kennis en ervaring (lessons learned) op het gebied van security awareness. Bijvoorbeeld door het bespreken van incidenten tijdens het werkoverleg.

eens      oneens  
5 4 3 2 1

10. Onze organisatie geeft alle medewerkers regelmatig opfriscursussen (gemiddeld één keer per jaar) op het gebied van security awareness.

eens      oneens  
5 4 3 2 1

### Betrokkenheid: (werknemers staan achter het belang van security awareness)

11. Na een test of een security incident koppelt de leiding of de beveiligingsfunctionaris direct aan de betreffende medewerker(s) terug wat de resultaten of acties zijn.

eens      oneens  
5 4 3 2 1

12. Tijdens trainingen of bijeenkomsten komen recente voorbeelden van security incidenten aan de orde.

eens      oneens  
5 4 3 2 1

### Belang: (werknemers hebben er belang bij om security aware te handelen)

13. Alle medewerkers is verteld dat security awareness van belang is voor de eigen veiligheid, die van collega's en die van derden.

eens      oneens  
5 4 3 2 1

14. Een werknemer die binnen onze organisatie niet security aware handelt, krijgt direct een sanctie opgelegd.

eens      oneens  
5 4 3 2 1

### Beloning: (security aware gedrag wordt gestimuleerd)

15. Onze organisatie stimuleert de medewerkers met (niet)financiële beloningen om security aware te handelen.

eens      oneens  
5 4 3 2 1

16. Leidinggevend noemen situaties waarin medewerkers security aware gehandeld hebben als voorbeeld tijdens het werkoverleg of in functioneringsgesprekken.

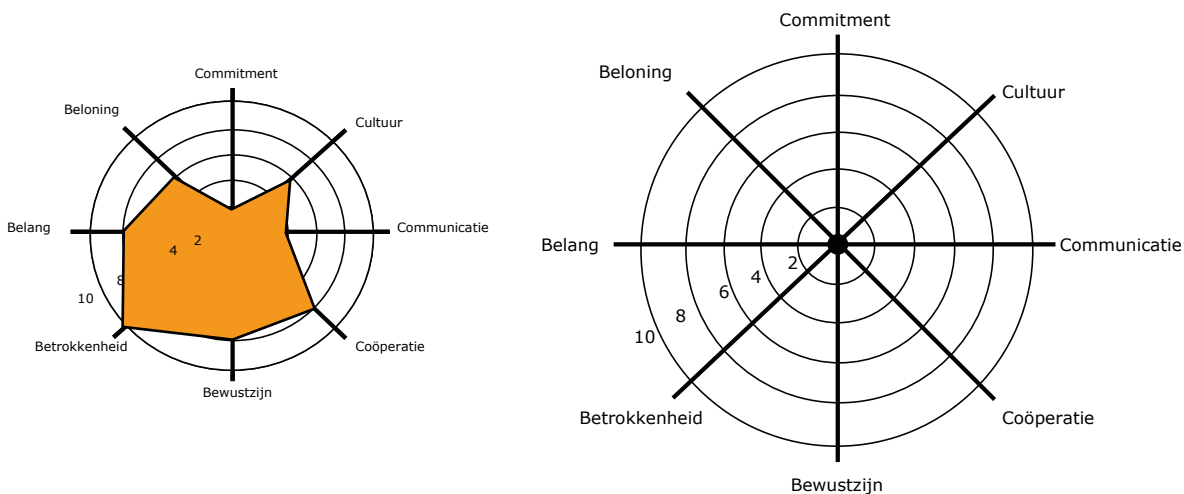
eens      oneens  
5 4 3 2 1

## Stap 2: Tel de scores op

Tel nu de antwoordscores van de vragen op per categorie en vul deze hieronder in. Vul vervolgens de scores in op de assen van het onderstaande cirkeldiagram. Verbind ten slotte deze punten met elkaar. Nu wordt zichtbaar op welke gebieden het security awareness programma in uw organisatie wellicht aandacht behoeft. De verschillende assen representeren de kritische succesfactoren van een effectief security awareness programma.

Commitment	Aantal punten	_____
Cultuur	Aantal punten	_____
Communicatie	Aantal punten	_____
Coöperatie	Aantal punten	_____
Bewustzijn	Aantal punten	_____
Betrokkenheid	Aantal punten	_____
Belang	Aantal punten	_____
Beloning	Aantal punten	_____
Totaalscore		_____

### Voorbeeld:



Is uw totaalscore lager dan 40, dan is aandacht voor security awareness in uw organisatie noodzakelijk. Een score tussen de 40 en 64 geeft aan dat uw organisatie één en ander goed geregeld heeft, maar dat er nog aandachtspunten zijn. Is uw score hoger dan 64, dan heeft uw organisatie voldoende aandacht voor security awareness. Wilt u meer weten over de kritische succesfactoren en de middelen die u in kunt zetten voor een effectief security awareness programma? Vraag dan het rapport 'Bekwaam in beveiligingsbewustzijn' aan (zie achterzijde). Voert u de quick scan uit met meerdere mensen, tel dan bij elke vraag de scores op en deel dat getal door het aantal deelnemers om per kritische succesfactor de gemiddelde waardering te krijgen. Zijn er grote verschillen in de beantwoording van een vraag, dan is dat een signaal om samen dieper in te gaan op de desbetreffende factor.

**Colofon**

Dit is een uitgave van de Nationaal Coördinator  
Terrorisbestrijding  
Postbus 16950 | 2500 bz Den Haag  
t 070 315 03 15

**Informatie**

Voor meer informatie over security awareness of het aanvragen  
van het rapport 'Bekwaam in beveiligingsbewustzijn' kunt u  
contact opnemen met de Directie Regie van de NCTb.