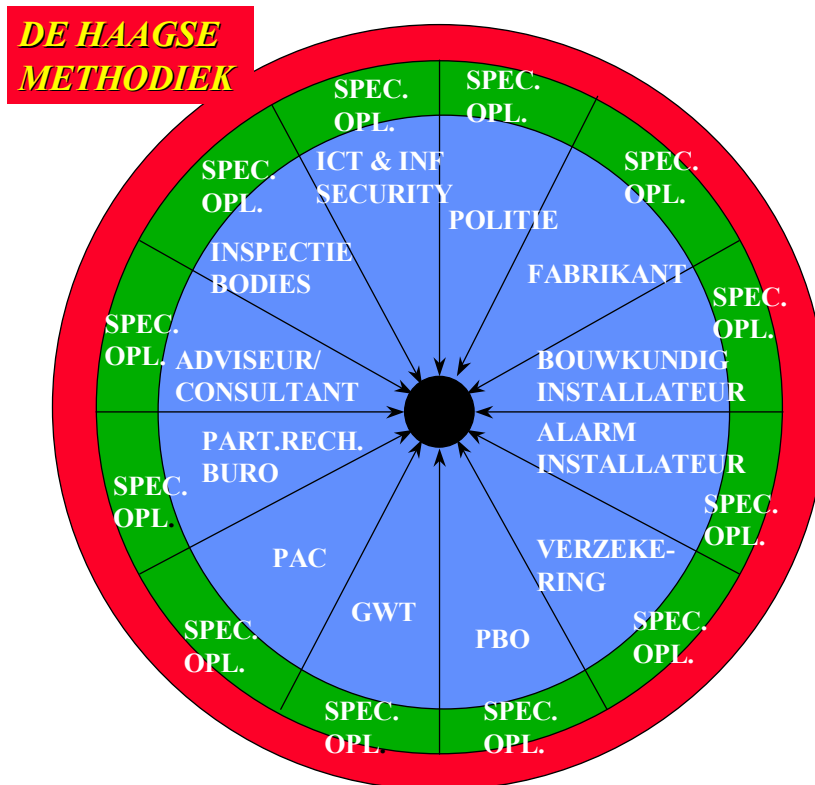


Introductie

DHM Security Management[®]



Alle rechten voorbehouden. Niets uit deze Introductie DHM Security Management® mag worden gereproduceerd door middel van boekdruk, foto-offset, fotokopie, microfilm of getranscribeerd of vertaald of welke andere methode dan ook, zonder voorafgaande schriftelijke toestemming van de auteurs. Van het materiaal in deze introductie mag geen gebruik worden gemaakt voor het geven onderwijs (waaronder begrepen: cursus, les, instructie, training e.d. welk recht de auteurs zich uitdrukkelijk voorbehouden.

DHM Security Management, De Haagse Methodiek (DHM), SBP (Security Beleidsplan), BSP (Basis Security Plan), BWP (Bewakingsplan), BSM (Bedrijf Security Manager), DHM-IBO (DHM plan Interne Beveiligingsorganisatie), DHM-EBO (DHM plan Externe Beveiligingsorganisatie), INCI/DEAR en PIP (Periodiek Inspectie Programma) zijn gedeponeerde merknamen. Gebruik ervan zonder voorafgaande toestemming van de merkhouders is niet toegestaan behoudens hetgeen hierna is toegestaan. Citeren van de hiervoor vermelde twee eerste merknamen in publicaties of op een internet website is toegestaan mits met verwijzing of een link naar de internet website: <http://www.dhm.nl> of <http://www.dhm-security-management.eu>.

Voor deelnemers aan een training/cursus gelden aanvullende voorwaarden welke bij inschrijving c.q. aanvang van de training/cursus worden verstrekt.

DHM Security Management[®] cursussen

Kennis van de DHM Security Management[®] methode gaat u verkrijgen door het volgen van een training/cursus DHM Security Management.

Dergelijke trainingen/cursussen geven wij, mr. R.C. Ackx RSE en ing. H.C.A. Duijndam RSE sinds 1994.

Doel

Doel van de cursus is u de voor het security proces noodzakelijke "DHM-tools" aan te reiken waarmee u een passend security management (basisniveau beveiliging) kunt opzetten en in stand houden en u te trainen in het gebruik van die "DHM-tools".

Doelgroep

DHM Security Management[®] richt zich tot alle actoren in de security branche, te weten: security/facility manager, Beveiligingsambtenaren (BVA) bij ministeries, security consultant, technisch inspecteur verzekeringsmaatschappij, manager particuliere Beveiligingsorganisatie, manager technisch beveiligingsbedrijf, manager inspectie body, politie-functionarissen (o.a. van het Bureau CCB), ICT-security officer, EBO-coördinatoren, Coördinatoren Integrale Veiligheid, etc.

Eindtermen

Aan het eind van de training/cursus bent u in staat mensen en middelen te managen die zijn ingezet voor het beheersbaar houden van incidenten welke de bedrijfsactiviteiten onbevoegd kunnen beïnvloeden.

Kern

Doel van de beveiliging¹ van bedrijven en instellingen is een gewenst niveau van veiligheid van personen en eigendommen te bereiken, bedreigingen of verstoringen van de continuïteit van de bedrijfsactiviteit en/of de omgeving tegen te gaan en op een geaccepteerd niveau te brengen en te houden. Kortweg: beveiligen tegen onbevoegde beïnvloeding van de bedrijfsactiviteiten.

Voor dat doel is de DHM Security Management[®], tevens bekend onder de naam De Haagse Methodiek (DHM)[®], ontwikkeld welke in Nederland inmiddels ruime bekendheid geniet.

Met de methode kan een passende beveiliging worden verkregen: van beleid tot en met uitvoering inclusief kwaliteitsborging. Tevens kan bereikt worden dat beveiliging methodisch en gestructureerd wordt opgezet en vervolgens planmatig plaatsvindt waardoor een grote mate van transparantie kan worden verkregen

Om te komen tot implementatie van DHM Security Management[®], dient in eerste instantie een interne security audit (ISA) uit te worden gevoerd. Na voltooiing daarvan kan het Security Management Pakket (SMP) worden opgezet en kan met het Periodiek Inspectie Programma (PIP) vinger aan de pols worden gehouden.

Met het ISA, SMP en PIP wordt u tijdens de training/cursus vertrouwd gemaakt.

Interne Security Audit (ISA)

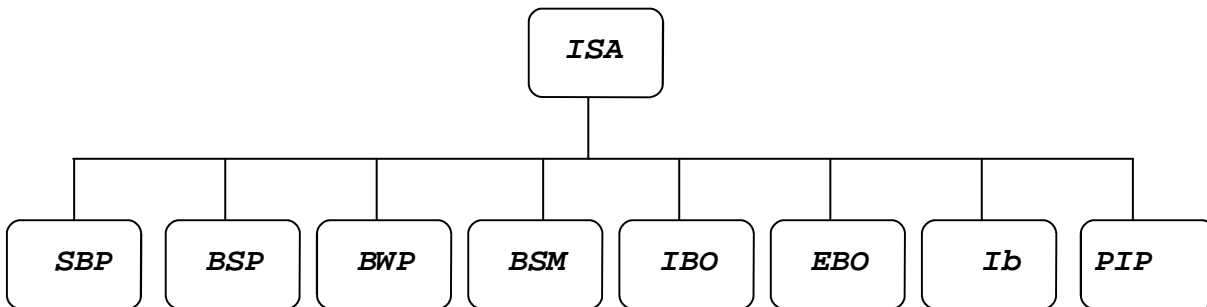
Tijdens de interne security audit (verder ISA genoemd) worden alle getroffen beveiligingsmaatregelen systematisch doorgelicht. Het verrichten van een dergelijke audit moet gezien worden als een normale activiteit in het kader van de kwaliteitszorg en in een kwaliteitszorgsysteem worden opgenomen.

Per risicoplaats² wordt nagegaan of de maatregelen voldoende beveiliging bieden tegen onbevoegde beïnvloeding van de bedrijfsactiviteiten.

¹ Beveiliging en security worden als zijnde synoniem in dit document gebruikt

² Risicoplaats = plaats waar zich een incident kan voordoen

Blijkt het laatste niet het geval te zijn dan worden voorstellen ter verbetering van de beveiliging gedaan. Bij het uitvoeren van de ISA volgens het DHM Security Management model wordt de NEN-EN-ISO 9001 als leidraad gehanteerd. In de vorm van een organogram ziet het ISA, dat u tijdens de cursus nog vaak zult terugzien, er als volgt uit:



Security Beleidsplan (SBP)

Aangezien security beleid de basis vormt voor security management en dus voor een optimale beveiliging, wordt tijdens de ISA in eerste instantie nagegaan of er adequaat security beleid is geformuleerd en vastgesteld door het management in de vorm van een Security Beleidsplan (SBP). Het betreft onder meer: verantwoordelijkheden, verwijzing naar relevante regelgeving en dreigingen waartegen beveiliging nodig wordt geacht.

Als nog geen SBP aanwezig is, wordt geadviseerd dit alsnog op te stellen.

Basis Security Plan (BSP)

Vanuit kwaliteitszorg is het noodzakelijk om een nulmeting te verrichten. Derhalve moet geïnventariseerd worden per risicoplaats geïnventariseerd:

- welk belang een risicoplaats vertegenwoordigt voor de betreffende organisatie,
- welke beveiligingsmaatregelen zijn getroffen, en
- wat de status van die maatregelen is.

De mogelijk te treffen beveiligingsmaatregelen worden onderscheiden in: organisatorische-, bouwkundige- en elektronische beveiligingsmaatregelen (de z.g. OBE-maatregelen).

Deze inventarisatie c.q. nulmeting vindt plaats met behulp van het BSP.

Bewakingsplan (BWP)

Het Bewakingsplan (BWP) dient om de relevante elementen te inventariseren van specifiek met bewakingstaken belast personeel, hun taken en bevoegdheden en de middelen die hen ten dienste staan.

Bedrijf Security Manager (BSM)

Vervolgens wordt nagegaan of iemand formeel is aangesteld als Bedrijf Security Manager binnen de organisatie. Een dergelijke (parttime) functionaris moet als focal point voor alle beveiligingszaken fungeren. Indien nog geen BSM is aangewezen wordt geadviseerd dat alsnog te doen.

Plan Interne /Externe beveiligingsorganisatie (Plan IBO / EBO)

De afhankelijk van het Risicoprofiel door de medewerkers van een bedrijf of instelling te nemen actie ingeval van een dreiging of incident kunnen worden opgenomen in een plan Interne Beveiligingsorganisatie (plan IBO). De met externe response forces gemaakte afspraken inzake van hen te verwachten actie wordt opgenomen in een plan Externe Beveiligingsorganisatie (plan EBO). Tijdens de ISA wordt nagegaan of dergelijke plannen bestaan. Is dat niet het geval dan wordt nagegaan of dergelijke plannen nodig zijn en zo ja dan wordt geadviseerd die alsnog op te stellen.

Incident beheersbaarheidsbepaling (Ib-traject)

Bij het Incident Beheersbaar traject (Ib-traject) vindt een grondige analyse plaats van risico's, gevolgen, kwetsbaarheden en toereikendheid van OBE-maatregelen, met zo nodig voorstellen ter verbetering, wijziging of aanpassing van die maatregelen.

De op basis van een Risicoprofiel³ opgestelde reëel voorstelbare scenario's worden "toegepast" op de verscheidene risicoplaatsen.

De gevolgen van de scenario's worden per risicoplaats gewaardeerd met behulp van een incident waarderingschaal (Wi-schaal).

Vervolgens wordt nagegaan of de getroffen beveiligingsmaatregelen (geïnterpreteerd tijdens het opstellen van het Basis Security Plan) voldoende zullen zijn om het incident beheersbaar te houden. Het gewenste niveau van beheersbaarheid moet door het management worden bepaald.

Voor de verdere analyse biedt DHM Security Management[®] twee mogelijkheden. De z.g. "lange route", welke met name is bedoeld om het beveiligingsbewustzijn en de betrokkenheid binnen een organisatie te vergroten en de "korte route", waarmee snel de Incident beheersbaarheid kan worden geanalyseerd.

Indien blijkt dat de beveiliging op bepaalde risicoplaatsen onvoldoende zal zijn om het incident beheersbaar te houden, dan moeten additionele maatregelen worden voorgesteld. Het verwachte resultaat van die additionele maatregelen wordt onderbouwd met de Inci/Detar[®] tijdpadanalyse methode.

Het Ib-traject voorziet tevens in het bepalen van een prioriteitsvolgorde voor de verbetervoorstellen.

Toezicht en handhaving (PIP)

Als laatste onderdeel van de ISA wordt nagegaan of periodiek een systematische en planmatige inspectie van de aanwezige beveiligingsvoorzieningen plaatsvindt.

Indien dat niet het geval is, wordt geadviseerd alsnog daarvoor een programma op te zetten. DHM Security Management[®] biedt daarvoor het Periodiek Inspectie Programma (PIP).

Security Management Pakket (SMP)

Nadat de beveiliging is opgezet volgens DHM Security Management[®] is het van belang om een complete en actuele beschrijving te hebben en te houden van alle getroffen beveiligingsmaatregelen. Dit kan in de vorm van het Security Management Pakket (SMP) dat alle hiervoor bij de ISA genoemde onderdelen bevat. Van het SMP wordt gebruik gemaakt bij de volgende ISA.

Nadere informatie en contact gegevens

Voor nadere informatie en contact gegevens wordt verwezen naar de website: <http://www.dhm.nl>.

* * * * *

³ Risicoprofiel betreft het overzicht van de risico's waartegen de organisatie zich wenst te beveiligen
Introductie DHM Security Management aug 2009