Whitepaper Security Management Systemen in Nederland

De coronacrisis houdt menig professional binnenshuis, vandaar dit initiatief.

Beveiliging als onderdeel van risico management wordt in veel organisaties verschillend geïmplementeerd. Vaak is die beveiliging gebaseerd op breed gedragen 'industry best practices'. Sommige van deze best practices zijn goed gedocumenteerd en worden gecontroleerd toegepast. Als een aanpak verschillende aspecten van het beheren van een organisatie bevat spreken we van een management systeem.

In deze whitepaper zijn 20 Security Management Systemen (SMS) geïnventariseerd en kort getypeerd die in Nederland veel worden toegepast. Met deze inventarisatie kunnen managers beoordelen welk SMS de organisatie voor implementatie kan overwegen.

Deze whitepaper is in maart 2020 als concept via de website www.spitsecurity.nl en via LinkedIn verspreid. Graag verneem ik uw aanvullingen, correcties en suggesties voor verbeteringen via een email of via LikedIn.

In juli zal een geactualiseerde versie verschijnen met een kort resume van de ontvangen reacties.

Dank voor je medewerking en wellicht tot ziens in beter tijden.

Met vriendelijke groet,

Marcel Spit

	Naam (kort)	Branche	Wet	Training	Bereik	Groei	Blz.	Taal	D.d.	Prijs[1]
1.	ABDO 2019	Defensie	Ja	Nee	Beperkt	Nee	182	NL EN	2017	gratis
2.	AEO	Exporteurs	Douanewet	Nee	Modaal	Ja	16	NL EN	2006	gratis
3.	BIO	Overheidsinformatie	Ja	Indirect	Groot	Nee	80	NL	2019	gratis
4.	BRC Food Safety	Voedselverwerking	Indirect	Nee	Groot	Nee	117	EN	2018	gratis
5.	CWA 15374	Beveiligd drukwerk	Nee	Nee	Beperkt	Nee	18	NL	2005	65,-
6.	DHM	Organisaties	Indirect	Ja	Groot	Ja	…	NL	2019	3.200,-
7.	IAEA	Nucleair	Kernenergiewet	Ja	Beperkt	Nee	57	EN	2011	gratis
8.	ICAO Annex 17	Luchtvaart	Luchtvaartwet	Ja	Groot	Nee	56	NL	2017	40.-
9.	IFS Food	Voedselverwerking	Indirect	Ja	Groot	Nee	158	NL EN	2017	gratis
10.	ISO 14298	Beveiligd drukwerk	Nee	Nee	Beperkt	Nee	20	EN	2013	130,-
11.	ISO 18788	Beveiligingsoperaties	Nee	Nee	Beperkt	Nee	98	EN	2016	220,-
12.	ISO 22301	Bedrijfscontinuïteit	Indirect	Ja	Modaal	Ja	36	EN	2014	160,-
13.	ISO 27001	Informatie	Indirect	Ja	Groot	Ja	37	NL EN	2017	150,-
14.	ISO 28000	Logistiek	Indirect	Nee	Beperkt	Ja	16	EN	2007	100,-
15.	ISPS Code	Havens	Havenwet	Ja	Groot	Nee	140	NL EN	2012	300,-
16.	KVO	Bedrijfsterreinen	Nee	Ja	Modaal	Ja	46	NL	2015	gratis
17.	MIVH	Hoger onderwijs	Nee	Nee	Beperkt	Nee	97	NL	2017	gratis
18.	SMS Norm 2017	Organisaties	Nee	Nee	Beperkt	Ja	50	NL EN	2017	16,-
19.	TAPA	Transport	Indirect	Ja	Beperkt	Nee	37	EN	2017	gratis
20.	VRKI / BORG	Bedrijven en huizen	Nee	Ja	Groot	Ja	23	NL	2019	gratis

Tabel met Security Management Systemen (SMS) die in Nederland worden toegepast

De meeste normatieve documenten zijn actueel en er wordt in Nederlandse wetgeving direct of indirect naar verwezen. Voor het implementeren en certificeren van verschillende van deze SMS'en zijn geregistreerde opleidingen en certificeringsschema's beschikbaar. De branche (toepassingsgebied), het bereik (mate van toepassing), de potentiele groei (ruimte in de markt) en de omvang, actualiteit (versie datum) en prijs van de normdocumenten verschillen zeer.

Hierna volgt een beknopte uiteenzetting van de verschillende SMS'en.

[1] Prijzen zijn afgerond en inclusief Btw per juli 2019

1. Algemene Beveiligingseisen Defensieopdrachten (ABDO) 2019

De Algemene Beveiligingseisen Defensieopdrachten 2019 bevat beveiligingseisen voor bedrijven die voor het Ministerie van Defensie aan gerubriceerde opdrachten willen werken. Het gaat om de beveiliging van Te Beschermen Belangen (TBB) van Defensie die buiten de Rijksoverheid worden gebracht. De ABDO 2017 is mede gebaseerd op nationale en internationale wet- en regelgeving, zoals de Wet op de inlichtingen en veiligheidsdiensten, de Wet veiligheidsonderzoeken, de Wet bescherming staatsgeheimen en de Archiefwet.

De ABDO is een nadere uitwerking van o.a. de ISO 270001 en het 'Voorschrift Informatiebeveiliging Rijksdienst voor de beveiliging van (bijzondere) Informatie' (VIR en VIRBI). De afdeling Industrieveiligheid van de MIVD adviseert en ziet toe op de naleving van de eisen uit de ABDO. Tijdens een ABDO-inspectie wordt daarom vastgesteld of voldoende zekerheid bestaat dat een adequate beveiliging is gewaarborgd.

Een PDF-versie is te vinden op https://www.defensie.nl/downloads/beleidsnota-s/2020/02/04/abdo-2019 [2]

2. Authorised Economic Operator (AEO)

De eisen om aan de AEO te voldoen staan o.a. in het Werkdocument 'HET AEO-COMPACT-MODEL' TAXUD/2006/1452 van de Europese Commissie. Het AEO COMPACT (Compliance Partnership Customs and Trade) Model van de Douane is een kader voor risicobeoordeling van goederenstromen. Met dit model kunnen de administratieve organisatie en de interne controle van een bedrijf worden beoordeeld. Een AEO Certificaat kan door de Douane wordt afgegeven aan bedrijven die aan een aantal veiligheidscriteria voldoen. Het certificaat biedt bedrijven voordelen in het internationale handelsverkeer, zo worden ze bijvoorbeeld minder streng gecontroleerd bij grensoverschrijdende handel. Deze bijzondere vorm van Supply Chain Security is onderdeel van Europese douanewetgeving.

Een PDF-versie is te vinden op https://download.belastingdienst.nl/douane/docs/aeo_compact_model_nl_do1781z1fd.pdf

3. Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (voorheen de BIR, BIG en BIWA) is per 1 januari 2019 verplicht voor de gemeenten, waterschappen, provincies en (in het interbestuurlijk verkeer met) het Rijk. De BIO is een gemeenschappelijk normenkader, gebaseerd op de ISO 27001/2 voor de beveiliging van de informatie(systemen) inclusief een aantal verplichte maatregelen (security baseline).

Een PDF-versie is te vinden op https://cip-overheid.nl/media/1303/bio-versie-103.pdf

[2] De in dit rapport opgenomen links naar internetpagina's en pdf-bestanden zijn van vertrouwde websites gehaald. Het openen van deze links en downloaden van bestanden is echter altijd voor eigen risico.

4. BRC 8 (Food Safety)

De BRC Global Standard for Food Safety (versie 8) specificeert veiligheids-, kwaliteits- en operationele eisen voor een managementsysteem voor een voedselverwerkend bedrijf. Beveiliging heet in deze norm 'Site Security en Food Defense'. Het gaat dan zowel over de beveiliging binnen het bedrijf, op het bedrijfsterrein en tijdens het transport. Security aandachtspunten zijn opleiding, dreigingsanalyse, risicoanalyse, insider threat, beveiligingsplan, incidentregistratie en -onderzoek, kwetsbare locaties (zoals opslag, innamepunten en open bewerking van grondstoffen en producten). Eisen worden gesteld aan toegangscontrole en -registratie, compartimentering, observatie en controles op grondstoffen of producten welke een bijzonder risico vormen. Ruimtes met significant risico's dienen te worden gedefinieerd, gemonitord en gecontroleerd.

Een PDF-versie is te vinden op https://www.brcgs.com/media/1316447/brc-global-standard-for-food-safety-issue-8-faqs.pdf

5. CWA 15374 Security management system for suppliers to the security printing industry

CWA 15374:2005 specificeert de eisen voor een SMS voor toeleveranciers van producten ter vervaardiging van waardedocumenten (zoals inkt, folie, stempels, hologrammen, gewaarmerkt papier). Deze CEN Workshop Agreement (CWA) is verouderd maar nog niet teruggetrokken.

ISO-, CEN- en NEN-normen zijn te bestellen in de NEN Shop: https://www.nen.nl/NEN-Shop/Security.htm

6. DHM Security Management

DHM Security Management®, ook bekend als De Haagse Methodiek (DHM), is een post-HBO Registeropleiding waarin cursisten een SMS leren te implementeren en te auditen. Onderwerpen zijn o.a. beleid, organisatie, risicoprofiel, scenario's, tijdpadanalyse, beveiligingsplan, continuïteitsmanagement, interne audit, kwaliteitsborging en inspectie.

Een brochure over DHM is te vinden op http://dhm.apollo.business/clientdata/105/media/pdf/DHM-leaflet-20190215.pdf

7. IAEA Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities

Deze aanbevelingen van de IAEA (met referentie INFCIRC/225/Revision 5) voor een SMS, aangeduid als: Operators' Physical Protection System is onderdeel van een serie publicaties van de IAEA over veiligheid van de nucleaire industrie. De handleiding is bedoeld voor overheden en operators van nucleaire installaties. Onderwerpen zijn o.a. beleid, verantwoordelijkheden, planning, beveiligingsplan, cultuur, coördinatie, dreigingsanalyse, risicomanagement, maatregelen, schillen, transport, respons, incidentafhandeling, inspectie, security baseline, continuïteitsmanagement en kwaliteitsborging.

Een PDF-versie is te vinden op http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf en een handleiding voor de implementatie op http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1849_web.pdf

8. ICAO Annex 17, Security

De volledige titel is Annex 17, Security — Safeguarding International Civil Aviation Against Acts of Unlawful Interference. Deze bijlage (annex) bij de Convention on International Civil Aviation (ICAO) bevat eisen en aanbevelingen voor de beveiliging van de burger-luchtvaart. Naast regelingen op (inter)nationaal niveau zijn veel onderdelen van een SMS voor luchthavens en luchtvaartbedrijven opgenomen. Onder andere de volgende onderwerpen van een SMS (zogenaamd Aviation Security Systems) zijn opgenomen: beleid, verantwoordelijkheden, management, beveiligingsplan, coördinatie, samenwerking, dreigingsanalyse, beveiligingsmaatregelen, toegangscontrole, bagage, cyber, in-flight security, kwaliteitsborging, audit, inspectie, incidentafhandeling en respons.

Een PDF-versie is te vinden op http://dgca.gov.in/intradgca/intra/icao%20annexes/an17_cons.pdf

9. IFS Food – Norm voor audits van kwaliteit en voedselveiligheid van voedingsmiddelen

IFS Food stelt eisen aan het voedselveiligheidssysteem voor bedrijven in de voedselverwerkende industrie. Een specifiek deel is gewijd aan beveiliging (Food Defense). Onderdelen van het SMS zijn: verantwoordelijkheden, planning, dreigingsanalyse, risicoanalyse, kwetsbaarheidsanalyse, beveiligingsplan, toegangscontrole, kwaliteitsborging, training en audit.

Een PDF-versie is te vinden op https://www.ifs-certification.com/images/standards/ifs_food6_1/documents/standards/IFS_Food_V6_1_nl.pdf

Een handreiking is te vinden op https://www.ifs-certification.com/images/standards/ifs_food6/documents/IFS_Food_DefenseGL_eng_web.pdf

10. ISO 14298 Beheer van processen voor beveiligd drukwerk

ISO 14298:2013 met oorspronkelijke titel is Management of security printing processes is (behalve de titel) niet naar het Nederlands vertaald. De norm specificeert eisen voor een SMS voor de producent van beveiligd drukwerk. Onderdelen van het SMS zijn o.a.: beleid, verantwoordelijkheden, Plan-Do-Check-Act-cyclus, audit, kwaliteitsborging en documentatie.

11. ISO 18788 Managementsystemen voor private beveiligingsoperaties

ISO 18788:2016 met oorspronkelijke titel Management system for private security operations is (behalve de titel) niet naar het Nederlands vertaald. De norm specificeert eisen en richtlijnen voor het inrichten van een Security Operations Management System (SOMS) voor het managen van private beveiligingsoperaties (zoals bewapende persoonsbeveiliging in risicogebieden). De norm refereert o.a. aan het Montreux Document on Pertinent International Legal Obligations and Good Practices for States, in relatie tot 'Operations of Private Military and Security Companies during Armed Conflict' en aan de uitgangspunten en afspraken opgenomen in het 'International Code of Conduct for Private Security Service Providers (ICoC)'.

12. ISO 22301 Managementsystemen voor bedrijfscontinuïteit

ISO 22301:2014 met oorspronkelijke titel: Business Continuity Management Systems (BCMS) specificeert eisen aan een continuïteitmanagementsysteem. Onderdelen van het managementsysteem zijn o.a. beleid, verantwoordelijkheden, Plan-Do-Check-Act-cyclus, impactanalyse, maatregelenplan, audit, kwaliteitsborging en documentatie.

13. ISO 27001 Managementsystemen voor informatiebeveiliging

De ISO 27001:2017 bevat eisen voor een Information Security Management System (ISMS) in het kader van de informatie-bedrijfsrisico's van een organisatie. De norm bevat mogelijke beheersmaatregelen en implementatiemaatregelen (zogenaamde 'controls'). Daarnaast zijn er nog verschillende normen in de ISO 27000-serie, zowel eisen-stellend als adviserend, en zowel op niveau van management systeem als op niveau van 'controls'. Onderdelen van het ISMS zijn o.a. beleid, verantwoordelijkheden, Plan-Do-Check-Act-cyclus, risicoanalyse, beveiligingsplan, toegangsbeheer, audit, kwaliteitsborging cyber en documentatie.

14. ISO 28000 Specificatie voor veiligheidsmanagementsystemen voor de logistieke keten

ISO 28000:2007 met oorspronkelijke titel Supply Chain Security is (behalve de titel) niet naar het Nederlands vertaald. De norm specificeert de eisen voor een SMS voor organisaties werkzaam in de logistieke keten. Onderdelen van het managementsysteem zijn o.a. beleid, verantwoordelijkheden, Plan-Do-Check-Act-cyclus, impactanalyse, maatregelenplan, audit, kwaliteitsborging en documentatie.

ISO-, CEN- en NEN-normen zijn te bestellen in de NEN Shop: https://www.nen.nl/NEN-Shop/Security.htm

15. ISPS Code voor de Beveiliging van Schepen en Havenfaciliteiten

De Internationale Code voor de Beveiliging van Schepen en Havenfaciliteiten (International Ship and Port facility Security Code, ISPS-code) van de Internationale Maritieme Organisatie (IMO) specificeert eisen voor de beveiliging van schepen en havenfaciliteiten. Onderdelen van de code zijn o.a. beleid, verantwoordelijkheden, taken, detecteren van bedreigingen, risicoanalyse, preventieve maatregelen, beveiligingsplan, security baselines (3 niveaus), toegangscontrole, bewaking, toezicht, audit, communicatie, alarmering, toetsing, oefening en training.

Een PDF-versie is te vinden op http://www.posec.nl/contents/nl/ISPS%20code%20Nederlandse%20versie.pdf

16. Keurmerk Veilig Ondernemen (KVO)

Het Keurmerk Veilig Ondernemen van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) verbetert op een gestructureerde manier de veiligheid van winkelgebieden en bedrijventerreinen. Centraal staat de samenwerking tussen ondernemers, gemeente, politie en brandweer. Onderdelen van het keurmerk zijn o.a. beleid, samenwerking, veiligheidsanalyse, risicoanalyse, beveiligingsplan, planning, (overval)preventietrainingen, toegangsbeheer, braakwerendheid, detectie, alarmopvolging, openbare verlichting, (camera)toezicht en brandpreventie, evaluatie, incidentafhandeling, cyber en kwaliteitsborging.

Een PDF-versie van het Handboek is te vinden op https://www.hetkeurmerkveiligondernemen.nl/fileadmin/user_upload/handboek_kvo_2015.pdf

17. Managementsysteem Integrale Veiligheid Hoger Onderwijs

Deze norm specificeert eisen voor een SMS voor onderwijsinstellingen op de volgende thema's: crisismanagement, informatie, privacy, kennisveiligheid, internationalisering, gebouwveiligheid, bhv, sociale veiligheid, integriteit, Arbo en milieu. Het integrale SMS bestaat uit o.a. de volgende onderdelen: beleid, leiderschap, competenties, verantwoordelijkheden, bewustzijn, Plan-Do-Check-Act-cyclus, dreigingsanalyse, risicoanalyse, beveiligingsplan, toegangsbeheer, audit, cyber, kwaliteitsborging, volwassenheidsniveaus en documentatie.

Een PDF-versie is te vinden op http://integraalveilig-ho.nl/wp-content/uploads/Management-Systeem-Integrale-Veiligheid.pdf

18. Security Management Systeem Norm 2017

Deze norm specificeert eisen en handreikingen voor het implementeren en beheren van een SMS voor alle organisaties. De norm is ook in het Engelse verkrijgbaar onder de titel: Universal Security Management Systems Standard 2017. Naast beveiliging zijn ook eisen opgenomen voor crisismanagement, continuïteitsmanagement, evenementbeveiliging, Arbo, Bhv en brand- en vluchtveiligheid. Het integrale SMS bestaat uit o.a. de volgende onderdelen: beleid, leiderschap, verantwoordelijkheden, taken, competenties, verwachtingen, bewustzijn, Plan-Do-Check-Act-cyclus, dreigingsanalyse, risicoanalyse, risicofuncties, kost- baten analyse, tijdpadanalyse, beveiligingsdoelen, beveiligingsplan, schillen, toegangsbeheer, audit, cyber security, kwaliteitsborging, security baseline, incidentafhandeling en documentatie. De norm maakt onderscheid in strategische, operationele, procedurele, organisatorische, tactische, fysieke en communicatie aspecten van beveiliging.

Een PDF-versie is te vinden op https://play.google.com/store/search?q=security%20management%20nsac&c=books

Een hard copy is te vinden op http://www.lulu.com/spotlight/Marcel_Spit

19. TAPA Facility Security Requirements (FSR)

Deze norm van de Transported Asset Protection Association (TAPA) specificeert eisen voor een SMS voor opslagfaciliteiten in de logistieke keten. Het SMS dat zich richt op de beveiliging van fysieke assets bestaat o.a. uit de volgende onderdelen: beleid, verantwoordelijkheden, risicoanalyse, screening, perimeter, hekwerken, CCTV, detectie, alarmopvolging, toegangsbeheer, schillen, sleutelbeheer, security baselines (3 niveaus), kwaliteitsborging en training.

Een PDF-versie is te vinden op https://www.tapa-global.org/fileadmin/public/downloads/FSR/TAPA_FSR_2017_Final.pdf

20. Verbeterde Risicoklassenindeling (VRKI)

De VRKI 2.0 van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is een instrument om op basis van het inbraakrisico gepaste beveiligingsmaatregelen te bepalen. Het geheel van deze maatregelen is als een basaal SMS te beschouwen. De beveiligingsmaatregelen bestaan o.a. uit organisatorische maatregelen, bouwkundige maatregelen, elektronische maatregelen, detectie, compartimentering, meeneembeperkende maatregelen, alarmtransmissie en respons.

Een PDF-versie is te vinden op https://hetccv.nl/fileadmin/Afbeeldingen/Certificatie-en-inspectie/Verbeterde_Risicoklassenindeling__VRKI_/VRKI_deel_A_januari_2019.pdf