Toezicht op de handhaving van fysieke securitymaatregelen

A. Koenders RSE

Bij het beheersen van de risico's zijn veel interne en externe functionaliteiten en partijen betrokken, zowel bij de inrichting als bij de instandhouding van de fysieke beveiliging binnen een organisatie. Op wat voor wijze beoordeelt de auditor de effecten van deze inspanningen?

Inleiding

Vele factoren en individuen spelen een bepalende rol in de beheersing van het veiligheidsproces, die alle – in meerdere of mindere mate – van invloed zijn op het resultaat. Hoe weeg je die resultaten en hoe bepaal je de efficiëntie en samenhang van de maatregelen?

Allereerst is het noodzakelijk om vast te stellen wat het doel van de genomen securitymaatregelen binnen de betreffende organisatie is. Securitymaatregelen behoren getroffen te worden in het kader van risicobeheersing. Het primaire doel is het waarborgen van de security en daarmee de continuïteit van de organisatie.
Risico's brengen veelal schade toe aan de goede naam van de organisatie en tasten wellicht de winstgevendheid aan; risico's zijn derhalve nadelig voor de continuïteit van de onderneming.

De continuïteit van een organisatie hangt dus af van een gezond evenwicht tussen:
1. de risicocomponenten die de organisatie kunnen bedreigen;
2. het scala aan maatregelen die zowel preventief als repressief genomen zijn om deze risico's te beheersen;
3. de aan die maatregelen verbonden kosten versus de omzet/winst.

In figuur 1 staan al deze componenten schematisch weergegeven op de 'continuïteitsbalans'.

Verklaring van het scala aan maatregelen

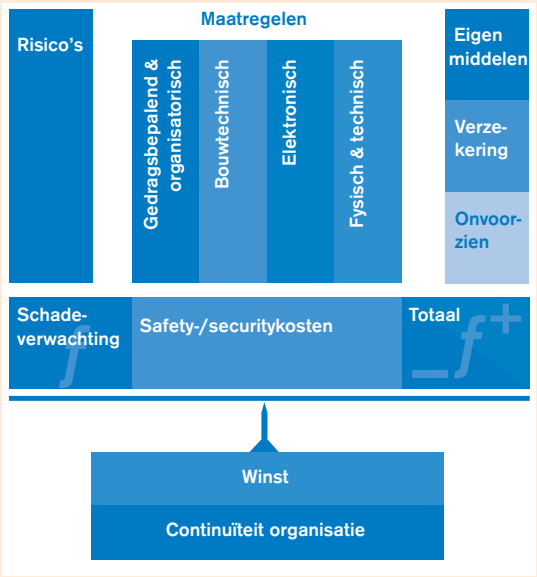
* Gedragsbepalende en organisatorische maatregelen
Gedragscode, beleidsstukken, procedures, richtlijnen, voorschriften, instructies, handboeken, controle- en rapportagerichtlijnen, aanwijzing verantwoordelijke functionarissen.

* Bouwkundige maatregelen
Materiële voorzieningen die tot doel hebben weerstand te bieden tegen het middelenarsenaal waarmee het onbevoegd binnendringen van een beveiligd object redelijkerwijs kan plaatsvinden. Zoals: muren, (brand)deuren, ramen, plafonds en daken.

* Elektronische maatregelen
Voorzieningen op elektronisch, elektrotechnisch en optisch gebied die een observerende, signalerende of alarmerende functie hebben. Zoals: closed circuit tv-systemen, infrarood detectoren en alarmcentrales.

* Fysische en ICT-maatregelen
Fysische beveiligingsmaatregelen zijn die maatregelen die binnen de organisatie getroffen zijn om met name de natuurkundige en chemische reacties die met de werkprocessen gepaard gaan, te beheersen en te controleren. ICT-maatregelen zijn die maatregelen die binnen de organisatie zijn getroffen om de vertrouwelijkheid, betrouwbaarheid en beschikbaarheid van ICT-systemen ten behoeve van de primaire processen te waarborgen.

Zoals uit figuur 1 blijkt, zijn de complexiteit qua werkprocessen en producten, de cultuur van de interne en externe disciplines en het veiligheidsbewustzijn van de betreffende organisatie dus belangrijke parameters bij de risicobeheersing.



Figuur 1. De 'continuïteitsbalans' van een organisatie.

Als interne disciplines kunnen bijvoorbeeld aangemerkt worden: (corporate) securitymanager, personeelszaken, security officer, interne accountantsdienst, facilitair bedrijf, eigen beveiligings- en bewakingsdienst, technische dienst, juridische zaken, bedrijfsgeneeskundige dienst, bedrijfshulpverlening, ondernemingsraad, salesmanager en productmanager.

Als externe disciplines kunnen bijvoorbeeld aangemerkt worden: politie, brandweer, overige hulpdiensten, particuliere alarmcentrale, particuliere beveiligingsorganisatie, recherchebureaus, fabrikanten, verzekeringsmaatschappijen, bouwkundige en technische installatiebedrijven, accountants en consultants.

Een belangrijke component voor de toetsing door de auditor is veelal niet het beleidskader maar meer het samenspel en de afstemming tussen de verschillende disciplines en verantwoordelijkheden met betrekking tot het totale veiligheidsproces. Een eenduidige gecoördineerde onderlinge communicatie is feitelijk het sleutelwoord en deze moet gebaseerd zijn op complete en betrouwbare securitymanagement- en stuurinformatie.

Interne auditactiviteiten

Ter verzekering van de doeltreffendheid van de beveiligingsmaatregelen dienen periodiek inspecties, interne security audits, selfassessments en ontruimings- en alarmoefeningen te worden uitgevoerd. De frequentie en aard van deze activiteiten dienen binnen het managementoverleg te worden overeengekomen en geagendeerd. Het spreekt voor zich dat hierbij rekening moet worden gehouden met de NEN-ISO-normen, uitgegeven door het Nederlands Normalisatie-instituut.
De bevindingen van de gehouden interne audits dienen te worden vastgelegd in separate rapportages ten behoeve van het management.

Externe auditactiviteiten

Het doel van de externe audit is het op onafhankelijke wijze laten beoordelen van de door de organisatie gekozen en geïmplementeerde veiligheidsmaatregelen en de daarbijbehorende interne audits en controles. De rapportage van de externe audit vergroot de garantie van een optimale waarborging van de kwaliteit van het scala aan veiligheidsmaatregelen voor de organisatie en kan zo nodig ook aan de (potentiële) relaties worden overhandigd.

Fysieke security audit

De auditor heeft als taak om de beheerorganisatie te toetsen qua opzet, werking en naleving. Daarbij controleert de auditor feitelijk de mogelijkheid tot en het daadwerkelijk handhaven van de securityregels, zoals vastgelegd in afspraken en beleid, binnen die organisatie. Doorgaans wordt een dergelijke toetsing gedaan door middel van een fysieke security audit. De rapportage bevat een weergave van de door de auditor opgetekende bevindingen verkregen door eigen waarneming en interne interviews.

Het doel van de fysieke security audit is een antwoord te geven op de volgende vragen:
* Voldoet het operationele pakket beveiligingsmaatregelen aan de door de organisatie gestelde normen en is deze gebaseerd op een adequate risico-inventarisatie?
* Is het pakket beveiligingsmaatregelen doeltreffend?
* Zijn er verbeteringen noodzakelijk en/of mogelijk en zo ja, binnen welke onderdelen en op welke wijze?

Een audit kan twee vormen hebben:
* *preventief:* analyse van de situatie vóór een incident of gebeurtenis;
* *repressief:* analyse van de situatie ná een incident of gebeurtenis.

Een doeltreffend hulpmiddel bij een audit is de checklist: De zeven 'W's'. Deze elementen zijn bij zowel een preventieve als een repressieve audit of toedrachtsonderzoek te gebruiken; zie tabel 1.

	Audit Preventief	**Toedrachtsonderzoek** Repressief
Wie	Alle personen die direct betrokken zijn bij de veiligheidsmaatregelen	Alle personen die direct betrokken en/of getuige waren van de gebeurtenis
Wat	Aard van de risico's	Wat is er gebeurd?
Waar	Nauwkeurige vaststelling en omschrijving van de risicolocatie	Nauwkeurige vaststelling en omschrijving van de locatie waar de gebeurtenis heeft plaatsgevonden
Wanneer	Tijdstip van de audit	Tijdstip van de gebeurtenis
Waarom	Doelstelling en motivatie van audit/ controle	Motief van veroorzaker of dader
Waarmee	Welke beheersingsmaatregelen?	Waarmee is het feit gepleegd?
Wijze	Op welke wijze en volgens welke normen heeft men de veiligheidsmaatregelen bepaald en getroffen?	Welke werkwijze (modus operandi) heeft de veroorzaker of dader gehanteerd?

Tabel 1. De zeven 'W's'.

Waarborging kwaliteit

Door een gestandaardiseerde periodieke toetsing van het scala aan beveiligingsmaatregelen ontstaat er een kwaliteitswaarborging binnen een organisatie. Door de standaardisatie is benchmarking binnen de branche dan wel binnen gelijksoortige vestigingen mogelijk. Tevens zijn de eventuele positieve of negatieve invloeden van de geïnitieerde verbeteringsactiviteiten te identificeren. Op dit soort componenten zal een auditor eveneens zijn onderzoek richten.

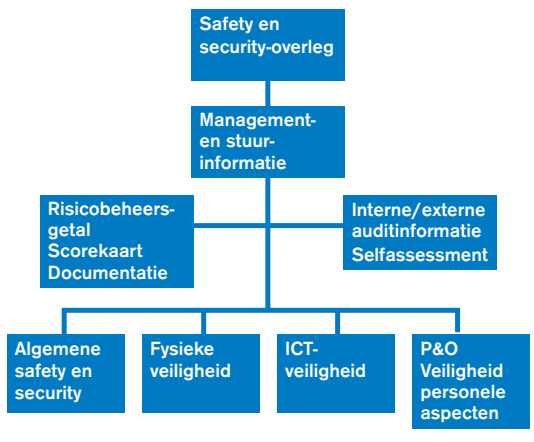
De beoogde kwaliteitsborging ontstaat met name als de verschillende disciplines die verantwoordelijk zijn voor de veiligheid, binnen het concern periodiek zorgen voor afstemming en overleg voeren (safety en security-overleg). Binnen dit overleg dienen de uitkomsten van in- en externe audits en van selfassessments, bij voorkeur geïntegreerd in een effectieve management- en stuurinformatiemethodiek, belangrijke input te vormen.

Het spreekt voor zich dat zo nodig de beveiligingsmaatregelen als gevolg van de bevindingen van de interne en/of externe audit worden bijgesteld, teneinde het gewenste beveiligingsniveau te kunnen (blijven) garanderen.

Na elke wijziging zal de betreffende documentatie moeten worden geactualiseerd en worden aangeduid door een adequaat versiebeheer. Op deze activiteiten zal door de coördinerende securityfunctionaris moeten worden toegezien.

Management- en stuurinformatie

Daar risico's tot financiële en imagoschade kunnen leiden, is het belangrijk dat het management kwalitatief en kwantitatief zicht krijgt op de gebeurtenissen. Als zich binnen een organisatie een onregelmatigheid heeft voorgedaan, is het door de differentiatie van verantwoordelijkheden op het managementniveau vaak onduidelijk wat er precies gebeurd is, wanneer en in welke omvang. De gegevens over de frequentie van soortgelijke incidenten zijn veelal ook niet voorhanden of snel te reproduceren. Er wordt uiteraard wel over incidenten en de gekozen oplossingen gerapporteerd, doch deze informatie is veelal zeer ad hoc en sterk incidentgericht. Veelal zijn het rapportages die zijn opgemaakt in de hitte van de strijd. Van het incident worden diverse separate rapportages opgemaakt, voornamelijk geënt op de specifieke verantwoordelijkheid van de verschillende functionarissen. Dan gaat het financiële deel naar de financieel directeur en de controller, gaan de technische aspecten naar het hoofd van de Technische dienst en de personele aspecten naar P&O. Ieder reageert sterk incidentgericht op de gebeurtenis en de samenhang van de preventieve en/of repressieve activiteiten wordt vaak onvoldoende belicht. Het effect van een ad-hocmaatregel is doorgaans verre van optimaal of echt afdoende om integraal gezien calamiteiten te voorkomen.
Registratie en rubricering van alle incidenten in een centrale incidentenregistratie bij de coördinerende securityfunctionaris draagt bij aan het inzichtelijk maken van de problematiek en het scala aan maatregelen. Het



Figuur 2. Elementen van kwaliteitsborging.

managen c.q. sturen door middel van een zogenaamde security scorekaart werkt daarom uitstekend binnen de veiligheidszorg. Door een dergelijke registratie:
* kunnen de voornaamste interne en externe bijzondere risico's van de organisatie en de genomen maatregelen op gestructureerde wijze in kaart worden gebracht;
* ontstaat er een raamwerk waarin de terminologie, systematiek en aanpak eenduidig zijn, opdat de informatie vergeleken kan worden, uitgewisseld en getoetst.

Door dit inzicht kan er ook beter over de informatie gediscussieerd worden en kan zo nodig het beleid bijgesteld dan wel opnieuw geformuleerd worden.

Security scorekaart

Een security scorekaart is een probaat hulpmiddel om de activiteiten van de verschillende disciplines in het veiligheidsproces te beheersen en te monitoren. Derhalve is zo'n instrument voor de auditor een uitstekend 'kompas' voor de toetsing van de handhavingsaspecten binnen die organisatie. Feitelijk geven de scorekaartindicatoren ook die elementen weer die een auditor normaliter ook toetst bij de beoordeling van het securityproces.

De gemeenschappelijke safety en security-attitude van de organisatie bepaalt haar veiligheidsgraad en continuïteit.

Hoe creëer je zo'n scorekaart en wat zijn belangrijke controlepunten? Het vervolg van deze paragraaf beschrijft in hoofdlijnen de belangrijkste componenten en illustreert die beschrijving met een gedeeltelijk uitgewerkt voorbeeld.
De componenten die in de scorekaart benoemd worden, behoren vanzelfsprekend gebaseerd te zijn op reële uitgangspunten en waarden. Over de keuzen en gestelde normen die in een security scorekaart worden weergegeven, dient met het oog op voldoende draagvlak consensus te bestaan binnen de verschillende disciplines. Immers, zij zijn ook voor de installatie en/of uitvoering van de maatregelen verantwoordelijk.

Teneinde de uitgangspunten niet tot een 'papieren tijger' te laten worden, zal het management ook consequenties moeten verbinden aan het wel of niet halen van de normwaarden. Dit kan zowel in een positieve als in een negatieve vorm van belonen (sanctie). Er dient immers altijd een prikkel te zijn om de normwaarden te halen. Handhaving zonder controle en sanctie is gedoemd te mislukken.

Voorbeeld 1. Samenspel tussen controle en sanctie.

Een kustplaatsgemeente die in de zomermaanden nabij het strand geen parkeerbonnen voor foutparkeerders door de politie laat uitschrijven, vraagt om een ondoordringbare verkeerschaos. Een tweede component in dit proces is de justitiële incasso. Als de uitgeschreven bekeuringen niet worden geëxecuteerd, heeft de bonnenschrijfactie ook geen resultaat. De repressieve handhaving inclusief sanctie maakt de situatie in dit voorbeeld beheersbaar. Het samenspel tussen de verschillende disciplines, namelijk politie en justitie, is ook beslist noodzakelijk daar de een niet zonder de ander kan. Immers, als er wel bonnen worden uitgeschreven, maar geen boetes worden opgelegd, leidt het uitschrijven van parkeerbonnen op de langere termijn niet tot het beoogde effect.

De normwaarden bij een security scorekaart behoren direct gekoppeld te zijn aan de beveiligingsdoelstellingen van de organisatie. Deze doelstellingen zijn dan ook bepalend voor de continuïteit en de winst van de organisatie.
Daar, zoals eerder gesteld, verschillende disciplines invloed hebben op het veiligheidsproces, zal de input voor de security scorekaart veelal ook door deze verschillende disciplines moeten worden aangeleverd. Het kan daarbij heel praktisch zijn dat elke discipline een eigen generieke scorekaart heeft, met specifieke items, welke uiteindelijk samenkomen tot een integrale scorekaart. Tezamen vormen deze scorekaarten de veiligheidsketen van de organisatie.
De input wordt bij voorkeur aangeleverd aan een centrale securitycoördinator. Een dergelijke functionaris is bij het samenspel van meerdere personen en afdelingen, bij wijze van katalysator en als 'spelverdeler', eigenlijk onontbeerlijk. Een security officer of (corporate) securitymanager kan zo'n coördinerende rol bij uitstek vervullen.
Het is mogelijk, maar dit is niet noodzakelijk, dat een dergelijke coördinator ook hiërarchisch geplaatst is boven de verschillende betrokkenen. Een en ander is sterk afhankelijk van de organisatiestructuur van het concern.

Opzet scorekaart

Voor het vervaardigen van een security scorekaart is het noodzakelijk om alle producten en diensten die zich binnen het veiligheidsproces manifesteren, te onderkennen. Deze elementen vormen immers tezamen een keten waarbij geldt dat de keten zo sterk is als de zwakste schakel. Feitelijk omvatten deze verschillende componenten de reden van het bestaan van een product, proces of afdeling.

Uit de security scorekaart blijkt tevens of de door de organisatie gestelde missie, doelen en strategie op koers liggen. De scorekaart vertaalt namelijk de missie en doelen in bestuurbare prestatie-indicatoren op meerdere perspectieven. Het hanteren van een security scorekaart geeft inzicht in de effecten van alle activiteiten van management en medewerkers die gevolgen hebben voor de scores op de prestatie-indicatoren. Verandering van de score op een indicator duidt erop dat het beter of slechter binnen het gedefinieerde securityniveau gaat. Zo helpt een scorekaart de organisatie zich te concentreren op die activiteiten die een bijdrage leveren aan het realiseren van de strategie, namelijk een gezonde graad van beveiliging.

Voor het totstandbrengen van een security scorekaart zullen de navolgende stappen uit de 'scorekaartcyclus' moeten worden doorlopen:
1. het inventariseren van de noodzakelijke activiteiten, inclusief het identificeren van de kritische succesfactoren (controlevariabelen);
2. het vaststellen van prestatie-indicatoren;
3. het meetbaar maken van prestatie-indicatoren;
4. het normeren van prestatie-indicatoren.

Voor de handhaving van de fysieke beveiliging van de organisatie zijn bijvoorbeeld de navolgende prestaties c.q. activiteiten noodzakelijk:
- Beveiligingscentrumactiviteiten
- Receptieactiviteiten
- Coördinatieactiviteiten
  a. Bewaking
  b. Beveiliging
- Kostenbeheersing
- Planning
- Advies
- Instructie
- Rapportage
- Surveillance- en controleronden
  preventief – toezicht op de werking van noodvoorzieningen (branddeuren, brandblussers, noodverlichting, enz.)
  repressief – toezicht op naleving beleidskaders (clear desk, parkeerbeleid, dragen ID-card, enz.)
- Bereikbaarheid
  a. telefonisch
  b. fysiek
- Calamiteitenbehandeling
- Incidentenbehandeling
- Incidentenregistratie
- BHV-activiteiten
- PAC-activiteiten (particuliere alarmcentrale)
- Zorg en beheer middelen en uitrusting
- EHBO
- Technisch beheer en uitvoering (Technische dienst)
- enzovoort.

Uit de doelstelling van de bovenstaande taken kunnen vervolgens de kritische succesfactoren en prestatie-indicatoren benoemd worden.
- *Kritische succesfactoren*:

Wat voor prestatie moeten we leveren om de gestelde doelen te realiseren?
- *Prestatie-indicatoren*:

Hoe meten we of en zo ja, in hoeverre we die doelen realiseren?

De prestaties c.q. activiteiten voor de security scorekaart kunnen bijvoorbeeld geënt worden op de navolgende vier perspectieven;
1. klant en markt;
2. proces;
3. financieel;
4. innovatie- en leervermogen.

Figuur 3 toont een gedeeltelijk uitgewerkte security scorekaart, waarin de eerste twee stappen uit de 'scorekaartcyclus' zijn opgenomen: controlevariabelen en prestatie-indicatoren.

Door de integrale benadering van de getroffen veiligheidsmaatregelen en het transparant visualiseren van de effecten van de inspanningen qua activiteiten en resultaten, krijgt de organisatie volledig inzicht in de status van de maatregelen qua opzet, werking en naleving.
Het is een continu proces en ook echt een teamsport waarbij alle disciplines even belangrijk en waardevol zijn.

Het is niet moeilijk voor een auditor om binnen een veiligheidsproces, dat slechts zelden de 'core business' van een organisatie vormt, leemten en manco's te vinden en te benoemen.
Het is veel lastiger om als coach die krachten op te roepen waardoor men binnen een evenwichtig en verantwoord budget gezamenlijk de veiligheidsketen optimaliseert en professionaliseert. Een proces waarbij de specifieke kennis van elke verantwoordelijke discipline de belangrijkste input vormt.
Een organisatie moet het nut en de noodzaak van haar inspanning inzien en onderschrijven, anders zal men zeker niet op effectieve wijze security-inspanningen plegen en er vervolgens op toezien dat de getroffen maatregelen worden gehandhaafd en nageleefd.
Zo niet, dan worden de gestelde criteria rond nooduitgangen alleen slechts binnen auditperioden gerespecteerd evenals de brandblusmiddelen qua aanwezigheid en deugdelijkheid worden gecontroleerd.

A. Koenders RSE
is werkzaam als adviseur bij KPMG Security Consulting. Daarvoor was hij onder meer security officer bij de Interne Accountantsdienst van Delta Lloyd. Ook werkte hij bij het Korps Rijkspolitie, district Amsterdam en was hij teamleider bij het team Schade Experts Algemene Dienst van Delta Lloyd Schadeverzekering N.V. De laatste drie jaar was hij actief met het opstellen en implementeren van een Integraal Veiligheidsbeleid voor het verzekering- en bankbedrijf als coördinator Criminaliteitsbeheersing bij Achmea.

Perspectieven	Controlevariabele	Indicator	Doelstelling	Norm
1 Klant en markt	* **klanttevredenheid**	score project, zaak evaluatie		
	* **productinnovatie** (leverbaarheid)	% wensen uitgevoerd binnen 40 dagen		
	* **klachten**	aantal mondeling/schriftelijk (bron = klager)		
	* **fouten** (die team kon voorkomen)	aantal fouten (steekproef, controle)		
	– communicatie			
	– behandeling (intern/extern)			
	– proces (juiste procedures volgen)			
	* **hit ratio** (opvolgen adviezen)	% opgevolgd en uitgevoerd		
	* **nakomen afspraken**	% nagekomen t.o.v. SLA/plan		
2 Proces	* **ontvangst en registratie bezoekers**	aantal aangemeld/niet aangemeld/garage		
	* **instructies**	productieaantal en wijzigingen		
	* **surveillance/ronden**	aantal ronden, aantal constateringen		
	* **afwikkeling incidenten**[1]	doorlooptijd		
	* **afwikkeling calamiteiten**[2]	doorlooptijd		
	* **rapportage**	aantal en aard		
	* **(beheersing) geweld**	preventief, repressief		
	* **technische alarmeringen**	aantal en aard		
	* **beveiligingsalarmeringen**	aantal en aard		
	* **telefonische bereikbaarheid**	aantallen, meting (telefooncentrale)		
	* **continuïteit**	aantal, gemiddelde duur onderbrekingen		
	* **beschikbare capaciteit**	productieve uren		
	* **storingen**	aantallen, aard, soort		
	* **adviezen**	aantallen afgegeven adviezen		
	* **teamtevredenheid**	teamenquête, % ziekteverzuim		
	* **speciale opdrachten**	doorlooptijd, aantal		
	* **clear desk-controles**	aantal, aard nalatigheid, locatie, frequentie		
3 Financieel	* **kostprijs diensten**			
	* **benutten capaciteit**			
	* **urenbesteding**			
	* **extra inzet** (kosten)			
	* **opleidingskosten**			
	* **kostprijs per FTE**			
4 Innovatie- en leervermogen	* **productverbetering**	aantal gerealiseerde actiepunten		
	* **procesverbetering**	– nieuwe rapportagevorm		
		– verbeteren procedures e.d.		
	* **opleiding** (kennisniveau)	% medewerkers opgeleid conform plan		
	* **cursus, examen, seminar**	aantal bestede uren		
	* **tijdsbesteding opleiding**	aantal opleidingsuren		

1) Bijvoorbeeld inbraak, diefstal, staande/aanhoudingen, brand (meldingen), vernieling/baldadigheid, fraude, bommelding, inzet politie en/of brandweer, vervanging defecte noodverlichting, blusmiddelen.
2) Bijvoorbeeld afpersing, bedreiging met de dood, smaad, ernstige verstoring van de continuïteit, bedrijfsongeval.

Figuur 3. Voorbeeld security scorekaart.