

NEN 7131: acht succesfactoren voor de implementatie van een organisational resilience management system

Joris Hutter

De nieuwe NEN 7131 'Organisational resilience management system' kan u helpen een systematische benadering van veiligheid in uw organisatie te implementeren. De norm richt zich op het vergroten van de veerkracht van de cruciale processen. Met de beschreven acht succesfactoren kunt u een grote sprong vooruit maken met uw hele organisatie of met een of meer afdelingen.

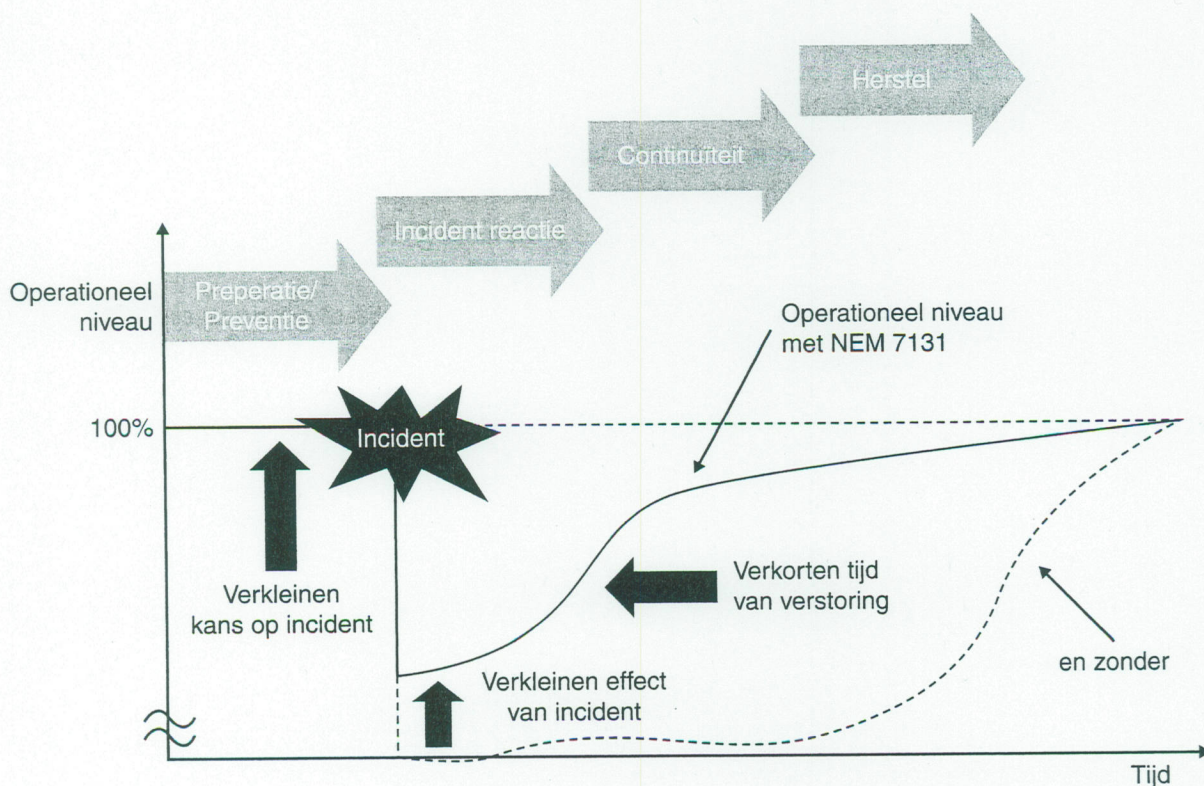
Ieder bedrijf en iedere instelling kent mensen die voorop lopen bij een systematische benadering van veiligheid en personen voor wie veiligheid geen belangrijke zaak is of alleen iets bij een incident. Bij afwezigheid van een systematische aanpak worden vaak alleen discussies gevoerd over maatregelen en niet over het doel van maatregelen. Als er al beleid is, mist dit vaak aansluiting met de bedrijfsdoelstellingen of met de praktijk. Met als resultaat dat er weinig waardering is door het hoger management en andere spelers en het onduidelijk is of het maatregelenpakket effectief is.

De nieuwe NEN 7131 'Organisational resilience management system' kan in deze situatie behulpzaam zijn. Met 'resilience' wordt de veerkracht bedoeld van de cruciale processen van de organisatie op versturende gebeurtenissen. Met deze norm wordt overigens weer een Engelstalig woord geïntroduceerd. U bent natuurlijk helemaal vrij om een ander woord voor 'resilience' te gebruiken. Ik ken een organisatie die de NEN 7131 als 'veiligheid management systeem (VMS)' introduceert, maar ik kan me voorstellen dat dit bij een andere organisatie weer verwarrend kan werken. Wij houden het hier voor de eenduidigheid op 'organisational resilience management systeem' ofwel ORMS.

In dit artikel wordt kort ingegaan waarop deze norm zich richt en hoe deze norm zich verhoudt tot andere managementnormen op het gebied van veiligheid. Belangrijker is de vraag welke stappen gezet moeten worden naar de invoering van een dergelijke visie in de organisatie. Wat moet u projectmatig doen om die aanpak in te voeren? Acht succesfactoren en noodzakelijke activiteiten die toegepast moeten leiden naar een succesvolle implementatie van een ORMS.

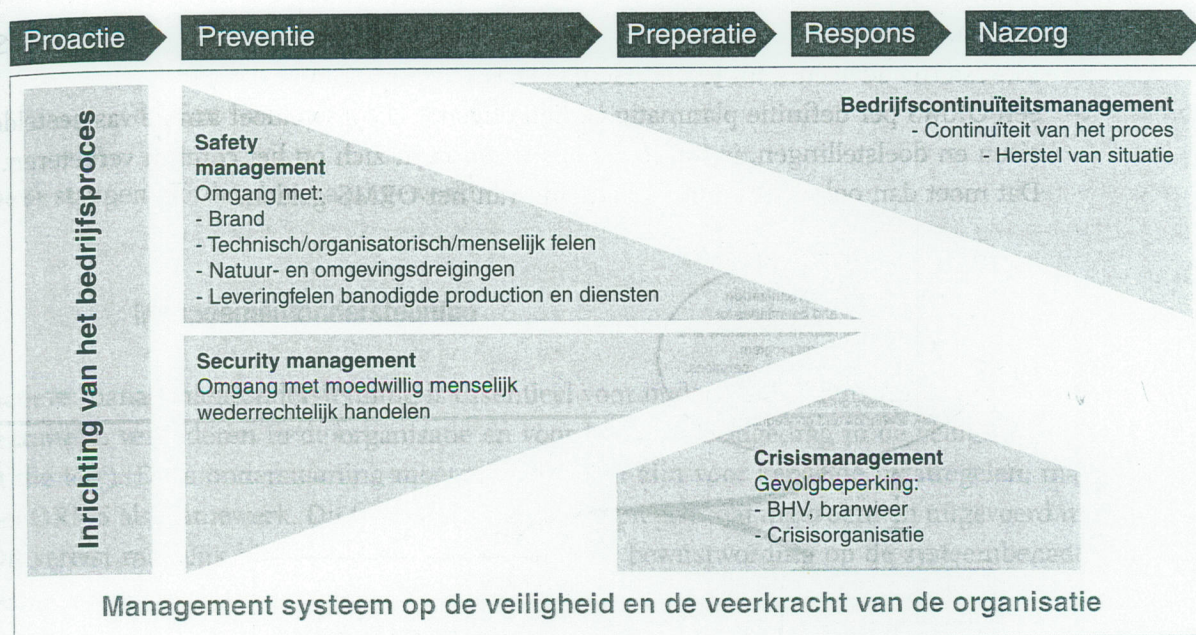
Waarop richt NEN 7131 zich?

NEN 7131 stelt bedrijven en instellingen in staat om aantoonbaar maatregelen te treffen voor het vergroten van de 'resilience' (veerkracht) van de cruciale processen. Dit wordt bereikt door samenhangende maatregelen te nemen op het voorkomen van versturende gebeurtenissen (= kansverkleining), op een adequate response op het incident (= effectverkleining) en op het beheersen van de gevolgen daarvan (= continuïteit van essentiële processen). Door een any-hazardbenadering worden in één managementsysteem security, safety en businesscontinuïteit met elkaar verbonden. Hierdoor ontstaat synergie in beleid en uitvoering en een effectieve communicatie met belanghebbenden.



Figuur 1. Werking van NEN 7131

NEN 7131 heeft als managementsysteem een Plan-Do-Check-Act-cyclus zoals NEN-ISO 9001 (kwaliteit), NEN-ISO 14001 (milieuzorg), OHSAS 18001 (arbo), NEN-ISO 22000 (voedselveiligheid), NEN-ISO 27001 (informatiebeveiliging) en NEN-ISO 28001 (supply chain security). Hierdoor wordt het voor de organisatie eenvoudiger om beleidsmatig en in uitvoering de sturing op operationele continuïteit (NEN 7131) te verbinden met andere veiligheids invalshoeken. Overigens is ook de nieuwe norm NEN-ISO 31000 interessant om voor de hele organisatie een vergelijkbaar risicomanagement-proces te hebben.



Figuur 2. Managementsysteem op de veiligheid en veerkracht van de organisatie

Naar implementatie van ORMS

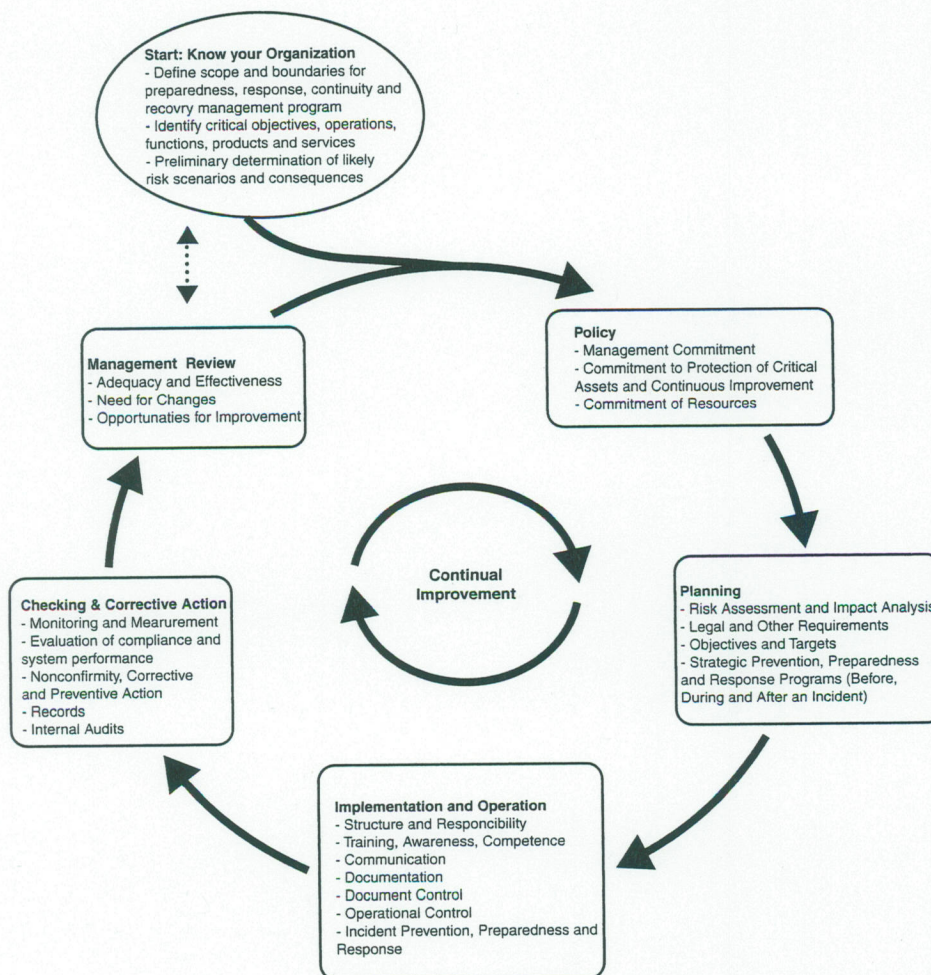
Een ORMS heeft mechanismen om de veiligheidsaanpak continu te verbeteren. Maar dat vliegwiel moet wel op gang gebracht worden

Invoering van een ORMS moet voorbereid worden en de implementatie kan het beste als een project aangestuurd worden. Daarbij moet men zich realiseren dat een ORMS een sociaal-organisatorisch systeem is waarbij geldt dat:

- het management invoering actief moet ondersteunen. Dit gebeurt alleen als het ORMS het management ondersteunt doordat het ORMS nauw gerelateerd is aan de organisatiedoelstellingen;
- in korte tijd resultaten bereikt moeten worden. Ieder managementsysteem stuurt op resultaten. Bij het kiezen van de scope van het ORMS en het opstellen van het projectplan moet het duidelijk zijn dat binnen enkele maanden concrete resultaten bereikt moeten zijn, zowel in de verbetering van de veiligheidssituatie als in de methodiek van het ORMS. Vaak is het zinvol om het ORMS eerst in één organisatieonderdeel of bij één proces in te voeren. Op basis van de successen en de leerervaringen kan het daarna breder worden ingevoerd of kan voor een hoger ambitieniveau worden gekozen;
- invoering van ORMS zo veel mogelijk gedaan wordt door personen die er daarna ook mee gaan werken. Dit betekent dat teamleden getraind moeten worden in de denkwijze van NEN 7131, waarna zij dit vertalen naar de risicobeheersing voor de eigen organisatie. Invoering is daarmee direct ook bewustwording en draagvlakcreatie bij de

stakeholders van het ORMS. Het heeft weinig zin om implementatie van het ORMS aan externe adviseurs uit te besteden;

- een ORMS per definitie planmatig is. Een effectief ORMS voldoet aan de vastgestelde eisen en doelstellingen, is intern consistent en richt zich op het continu verbeteren. Dat moet dan ook voor de implementatie van het ORMS gelden.



Organizational Resilience (OR) Management System Flow Diagram

Figuur 3. ORMS-vliegwiel

De volgende activiteiten moeten in relatie tot elkaar worden genomen:

1. Managementondersteuning zekerstellen.
2. Aansluiten op bedrijfs- en veiligheidssituatie.
3. Analyse maken van belangrijkste stakeholders.
4. Verduidelijken van doelstellingen en organisatorische inpassing ORMS.
5. Gap analysis uitvoeren.

6. Project afbakenen.
7. Rol van interne en externe medewerkers bepalen.
8. Een businesscase opstellen.

Deze stappen worden hierna uitgewerkt.

Managementondersteuning

Actieve managementondersteuning is essentieel voor budget, voor doorzettingsmacht om werkwijzen te kunnen veranderen in de organisatie en voor het voorbeeldgedrag in de veiligheidscultuur ('tone at the top'). Deze ondersteuning moet er niet alleen zijn voor bepaalde maatregelen, maar ook voor het ORMS als framework. Dit framework is 'the big picture' dat ingevoerd en uitgevoerd moet worden. Dit vereist mogelijk bij het management specifieke bewustwording op de systeembenadering van veiligheid en wat dat de organisatie te bieden heeft.

Ook moet uitgezocht worden wat de prioriteiten zijn van de directie op veiligheidgerelateerde issues. De scope van het ORMS, dan wel het invoeringsprogramma, kan hier op afgestemd worden.

Managementondersteuning gebeurt door initiatiefnemers te steunen in het voortraject van een ORMS en het naar buiten toe communiceren van het belang van veiligheid. De beslissing tot de implementatie van een ORMS zal daarna gebeuren op basis van een businesscase en een projectplan.

In sommige organisaties is het niet duidelijk bij wie in de directie veiligheid belegd is. Als dat zo is, moet u proberen de directie een van hun leden tot portefeuillehouder veiligheid te laten benoemen.

Aansluiten op bedrijfs- en veiligheidssituatie

Het ORMS en de prioritering van invoering moet aansluiten op de bedrijfssituatie. Dit moet in het beslisdocument tot uitdrukking komen. In wat voor bedrijfsomgeving bevindt de organisatie zich? Wat zijn de technologische ontwikkelingen? Hoe wordt in de bedrijfstak en bij het management naar risico's gekeken (risicotolerantie)? Wat zijn kenmerken van de geografische locatie? Kortom, het ORMS moet een heldere aansluiting hebben met de missie van de organisatie.

In de concretisering moet helder zijn wat de essentiële processen en bedrijfsmiddelen zijn van de organisatie, wie de essentiële klanten zijn, wat het effect is van interrupties van essentiële bedrijfsprocessen en wat consequenties kunnen zijn van aansprakelijkheid, contractuele verplichtingen en het niet voldoen aan wet- en regelgeving. Deze helderheid is nodig voor alle betrokkenen, anders verliest u het commitment (top-down) en de support (bottom-up) uit uw organisatie en het vertrouwen van externe belanghebbenden. Wat zijn mogelijk versturende gebeurtenissen en hebben die zich in het verleden in het eigen bedrijf of bij een vergelijkbare organisatie ook voorgedaan?

Zijn er in de bedrijfstak (internationale) standaarden die als vanzelfsprekend worden verondersteld? Ook de wijze van aansturing en verantwoording inzake veiligheid ('governance') moet aansluiten op de karakteristiek van het bedrijf of de instelling. Is deze centraal of juist decentraal?

Stakeholders

Maak een analyse van de belangrijkste stakeholders. Denk aan besluitvormers binnen de organisatie, opiniemakers, klanten en leveranciers (supply chain partners), medewerkers, personen die menen dat zij geraakt worden door veiligheidsbeslissingen, belangengroepen, financiers, verzekeraars, overheden, hulpdiensten of media.

Wat willen zij? Een directie zal over het algemeen niet geconfronteerd willen worden met risico's die door hen niet beheersbaar worden geacht. Een adequate rapportage op risico's is daarom veel waard. Iedere stakeholder heeft ook wat te bieden. De directie kan budget verstrekken en doorzettingsmacht bieden bij veiligheidsbeslissingen. Voor andere stakeholders liggen de belangen anders, evenals wat zij te bieden hebben bij een veilige bedrijfssituatie. Breng in kaart wat de verwachte communicatie per stakeholder is.

Doelstellingen en organisatorische inpassing

Maak duidelijk wat de doelstellingen zijn van het ORMS en wat de organisatorische context is. Bijvoorbeeld:

- Wilt u de resilience-prestatie vergroten? Bijvoorbeeld door te voldoen aan regelgeving, standaards, een contract of aan risicobeperking.
- Wilt u met het ORMS de betrokkenheid bij veiligheid binnen de organisatie vergroten?
- Wilt u het zicht op de risico's vergroten? Wilt u de risico's beperken?
- Wilt u zicht hebben op de noodzakelijke kosten?
- Hoe verhouden de doelstellingen van het ORMS zich met de strategische doelstellingen van de organisatie?
- Wat zijn de juridische, politieke, culturele en sociaaleconomische factoren die in overweging moeten worden genomen?
- Wie zijn de stakeholders en wat is hun risicoperceptie?
- Hoe past het ORMS binnen de bredere planning- en aansturingprocessen van de organisatie?

Gap analysis

Voer een gap analysis uit om inzicht te krijgen in hoeverre de huidige werkwijze voldoet aan de criteria van de NEN 7131. Waaruit bestaan de huidige managementaanpak, procedures, beleid, trainingsprogramma's en andere factoren? Welk delen van de huidige werkwijze voldoen en welke hebben een verbetering nodig? Deze review kan bestaan uit interviews, checklijsten, inspecties, metingen, en uit eerder uitgevoerde reviews.

In de gap analysis moet in ieder geval aandacht zijn voor:

- identificatie van de kritische bedrijfsdoelstellingen, bedrijfsmiddelen, bedrijfsactiviteiten, producten en diensten van de organisatie en hoe deze zich verhouden tot de missie;

- identificatie van de risico's, waarbij aandacht is voor de normale bedrijfsomstandigheden, maar ook voor bijzondere bedrijfssituaties (welke bedrijfssituaties komen voor?);
- identificatie van de wet- en regelgeving en andere verplichtingen die de organisatie is aangegaan;
- onderzoek van de huidige risicomanagementpraktijken en -procedures, inclusief die door derden, bijvoorbeeld contractors, worden uitgevoerd;
- evaluatie van eerdere incidenten, ongelukken en noodsituaties.

Projectafbakening

Maak de projectafbakening. Op welke bedrijfsactiviteiten, organisatieonderdelen of risico-issues zal het ORMS worden ingericht? Maak een haalbare projectafbakening, opdat in enkele maanden resultaten zichtbaar zijn. Kies een organisatieonderdeel of bedrijfsactiviteit met managers die graag meewerken en waarbij het aantal betrokken personen relatief beperkt is. Daarmee kan in enkele maanden een managementsysteem volgens de NEN 7131-aanpak worden ingericht. Op basis van de ervaringen kan daarna besloten worden om de scope van het ORMS te verbreden naar andere bedrijfsprocessen, organisatieonderdelen of andere type risico's. Voor afbakening en inrichting geldt:

- Maak de afbakening niet te groot, opdat snel resultaten zichtbaar zijn.
- De afbakening moet wel wat om handen hebben en gerelateerd zijn aan de business en de prioriteiten van het management.
- Leg vast wat bereikt moet worden op risicobeheersing. De gap analysis geeft hiervoor het inzicht. Ook hier geldt dat de doelstellingen haalbaar moeten zijn. Het is bevredigender om bij de projectevaluatie de doelstellingen behaald te hebben en daarna te beslissen om de lat wat hoger te leggen, dan te moeten melden dat de doelstellingen niet gehaald zijn.
- Leg vast wat de doelstellingen zijn voor het ORMS en hoe het ORMS zich verhoudt tot hoe er in de organisatie op resultaten wordt gestuurd.
- Zorg voor steun van de directie en laat dat gecommuniceerd worden binnen de organisatie.
- Kies een proceseigenaar of een projectleider die succesvol is in de eigen organisatie. Dit moet een systeemdenker zijn (bijvoorbeeld affiniteit met ISO-9001 of ISO-14001).
- Kies teamleden uit de processen en afdelingen waar het ORMS betrekking op heeft. Mogelijk zijn dat ook personen van externe partijen als toeleveranciers en subcontractors.
- Verzorg een training voor alle projectleden op de principes en aanpak van een ORMS.
- Kies zo vroeg mogelijk een beheerder van het ORMS, voor het documentbeheer en andere beheertaken die ontstaan (bijvoorbeeld organisatie van overleg met stakeholders). De projectorganisatie op invoering van het ORMS kan daardoor met dezelfde personen glijdend overgaan naar een beheer- en uitvoeringsorganisatie van het ORMS.
- Zorg voor een kick-off waarin duidelijk wordt gemaakt wat de probleemstelling en doelstellingen zijn van het project, wat criteria en randvoorwaarden zijn, welke resultaten uit de gap analysis ingevuld moeten worden, wat het stappenplan is en wat ieders rol is.

- Het is effectiever om bij de implementatie van het ORMS, indien mogelijk, gebruik te maken van al bestaande procedures en structuren. Die zijn namelijk al geïntegreerd in de werkwijze van de organisatie en dat is nu precies de bedoeling van het ORMS.
- Communiceer met de relevante stakeholders voor en tijdens de implementatie.

Rol van training en van externe adviseur

Het doel van een ORMS is dat het bedrijf of de instelling zelf haar veiligheid effectief organiseert. Dat gaat niet lukken als de implementatie van het ORMS aan een externe adviseur wordt uitbesteed. Een extern adviseur kan bij het project meerwaarde hebben in een ondersteunende rol bij het verhelderen van de methoden, in het ondersteunen bij analyses en maatregelenselectie of bijvoorbeeld in een eerste structurering van documenten. Laat het merendeel van het werk echter doen door vertegenwoordigers uit de processen en zorg dat documentatiebeheer zo vroeg mogelijk wordt uitgevoerd door de toekomstig beheerder van het ORMS.

Training is belangrijk voor het slagen van de doelstellingen. Dit betreft inzicht in systeemdenken, inzicht in de structuur van NEN 7131 en methoden als risicoanalyse en maatregelenselectie. Het wordt daarna voor de projectleden veel eenvoudiger om de vertaalslag in de organisatie te maken.

Businesscase: kosten en baten van de invoering en instandhouding van ORMS

Stel een businesscase op, waarbij de volgende kostenposten betrokken kunnen worden:

- tijd van managers;
- tijd van medewerkers (is de bulk van de tijd);
- kosten van extern adviseur;
- kosten van externe training;
- kosten van de resilience-maatregelen zelf.

U kunt daar de volgende baten tegenover zetten:

- verbetering van de securityprestatie;
- vergroting van de compliance;
- risicoverkleining en verbeterde bescherming van de cruciale processen en middelen;
- nieuwe klanten/markten;
- vergroting van efficiëntie, verlaging van kosten;
- verbetering van moraal en vertrouwen van medewerkers;
- verbetering van imago naar publiek, regelgevers en financiers;
- verbetering van bewustzijn bij medewerkers op securityissues en verantwoordelijkheden.

Ten slotte

Soms lukt het om grote sprongen te maken, vaak moet je tevreden zijn met kleinere stappen. Als het niet voor de hele organisatie kan, implementeer het ORMS dan op bedrijfsunit- of afdelingsniveau. De referentieaanpak van NEN 7131 geeft handvatten om het veiligheidsmanagement direct te verbeteren en daarmee ook de kwaliteit van het proces of de afdeling. En als het op een beperkte schaal goed functioneert, is het wachten op het moment om het ORMS breder in de organisatie in te voeren.

Beveiliging Totaal

2012

Artikelen, Regelingen,
Producten, Adressen



Inhoud

I. Redactionele artikelen

Beveiliging

- | | |
|---|----|
| 1. Criminaliteit in Nederland
<i>Harry Eggen</i> | 17 |
| 2. Trends in overvallen
<i>Jos van der Stap</i> | 33 |
| 3. Winkeldiefstalpreventie: een gedragsbenadering
<i>Jeske Nederstigt</i> | 37 |
| 4. Ongewenst gedrag van de klant, er is wel degelijk een
aanpak voor: Trainingen in de detailhandel
<i>Evelien van Zuidam</i> | 49 |
| 5. Slim beveiligen
<i>Hidde de Jong</i> | 57 |
| 6. 'Lean Security'-alarmopvolging beschouwd door middel van Six Sigma
<i>Alfons Koenders</i> | 61 |
| 7. NEN7131: acht succesfactoren voor de implementatie van een
organisational resilience management system
<i>Joris Hutter</i> | 75 |
| 8. Information security verankeren in de organisatie
<i>Lotte van der Waa en Marc Burger</i> | 85 |
| 9. Beroepsmatige en wetenschappelijke (security management) titulatuur
<i>Ralph van Os MA</i> | 93 |