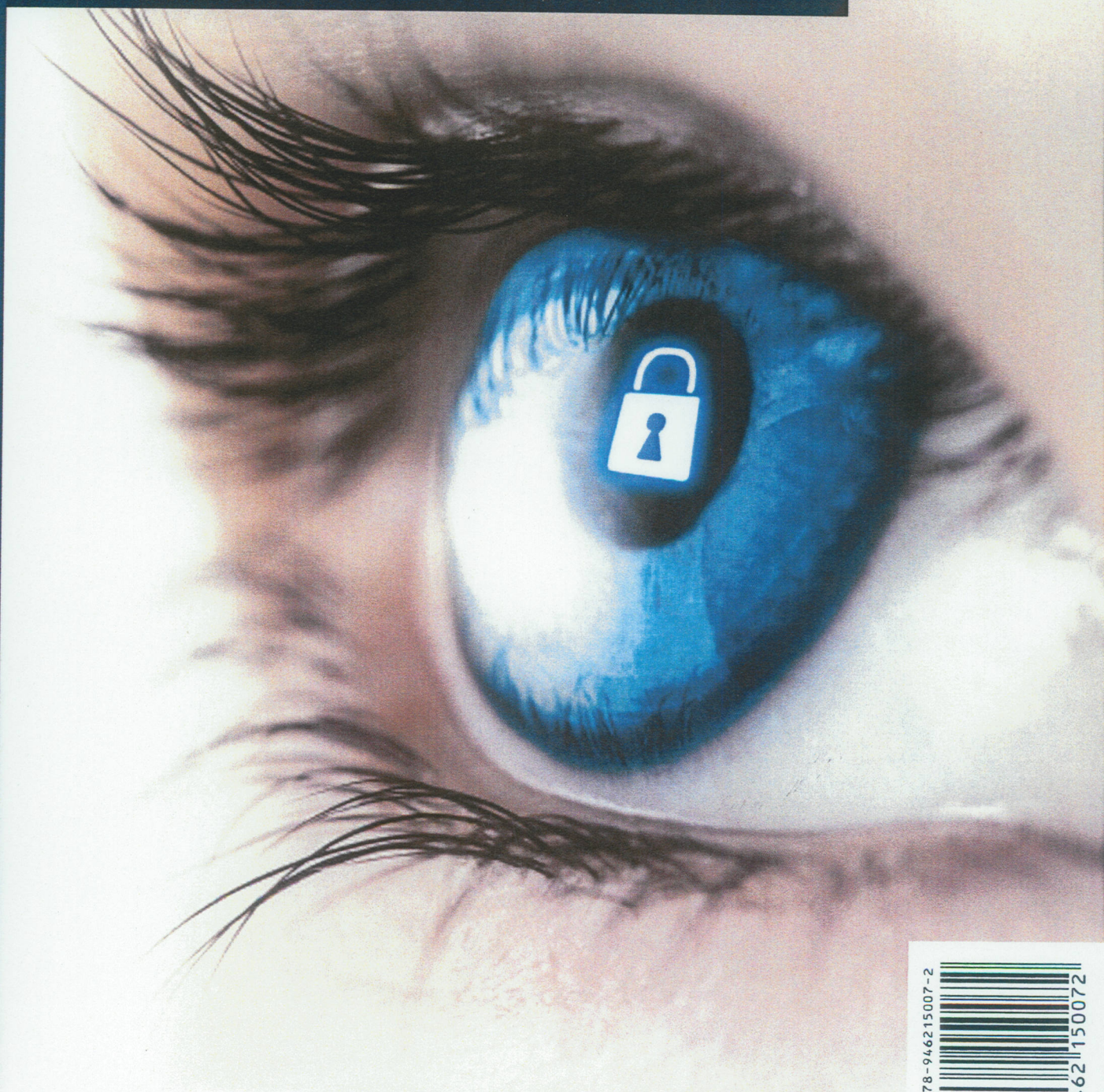


Beveiliging Totaal

2013

Artikelen, Regelingen,
Producten, Adressen



SECURITY Management

www.securitymanagement.nl

ISBN 978-946215007-2



9 789462 150072

Inhoud

I. Redactionele artikelen

Beveiliging

- | | |
|--|----|
| 1. Criminaliteit in Nederland
<i>Harry Eggen</i> | 17 |
| 2. Stand van zaken overvallen
<i>Jos van der Stap</i> | 31 |
| 3. Duurzame veiligheid
<i>Rob van Veen</i> | 39 |
| 4. Nieuwe ISO-norm voor bedrijfscontinuïteitsmanagement
<i>Joris Hutter</i> | 51 |
| 5. Predictive profiling
<i>Bert van Pel CSP</i> | 57 |
| 6. Compliance
<i>Alfons Koenders</i> | 65 |
| 7. Selectie van een particuliere beveiligingsorganisatie
<i>Olof Homoet RSE</i> | 77 |
| 8. Websitebeveiliging
<i>Sebastiaan van der Meer</i> | 87 |

Brandveiligheid

- | | |
|--|-----|
| 1. Brandweerstatistiek
<i>Mark Vlemmings</i> | 97 |
| 2. Grote branden en schadecijfers
<i>Leo Porrio</i> | 109 |

Nieuwe ISO-norm voor bedrijfscontinuïteitsmanagement

Joris Hutter

Een grote stroomstoring legt delen van het land plat. Een griepgolf ontwikkelt zich tot pandemie. Uw belangrijkste leverancier is door brand verwoest. Is uw organisatie in staat gewoon door te blijven werken? BCM, bedrijfscontinuïteitsmanagement, wordt voor veel organisaties steeds belangrijker. De nieuwe ISO-norm voor bedrijfscontinuïteit is vanwege zijn universele aanpak en het internationale draagvlak een goede basis om uw organisatie calamiteiten-proof te maken.

Inleiding

In mei 2012 is de ISO 22301 'Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit – Eisen' [auteur: aldus www.nen.nl] gepubliceerd. Dit is een volgende mijlpaal in de ontwikkeling van afspraken over hoe organisaties kunnen aantonen dat zij hun belangrijkste bedrijfsprocessen kunnen voortzetten na verstoringen. Deze norm voor bedrijfscontinuïteitsmanagement, of Business Continuity Management, kortweg BCM, is belangrijk voor de organisatie zelf, maar ook voor ketenpartners, toezichthouders en andere belanghebbenden.

Historie

Continuïteitsmanagement werd in eerste instantie gebruikt om de omgang met verstoringen van de ICT te waarborgen. Binnen de 'Code voor informatiebeveiliging' is continuïteitsmanagement dan ook een belangrijk onderdeel. Dit komt tot uitdrukking in de eisen stellende ISO 27001 en de *guide-line* hierop, ISO 27002. De afgelopen vijftien jaar kwam steeds meer aandacht voor systematisch plannen hoe de organisatie om moet gaan met verstoringen van de operationele continuïteit van de business. Grote organisaties ontwikkelden hiervoor eigen bedrijfsnormen. Daarnaast ontstonden algemene normen. In Nederland is waarschijnlijk de Britse norm BS 25999 de bekendste norm op het gebied van BCM. In 2011 en 2012 is vanuit ISO een proces doorlopen om vanuit de kennis van verschillende BCM-aanpakken een ISO-norm op te zetten. Belangrijke spelers hierbij waren norminstellingen uit Engeland (BS 25999), Australië, Singapore, Israël maar ook ASIS International. Inhoudelijk bevat de norm de kennis waarmee met de verschillende 'moedernormen' ervaring is opgebouwd. Dat is ook logisch, want al deze normen gaan over BCM.

Wat is nieuw aan ISO 22301?

Er zijn twee nieuwe aspecten aan de ISO 22301. Ten eerste het gedachtegoed dat nu één referentiekader bestaat voor BCM's, waardoor het toepassen en communiceren van eisen en aanpakken een stuk eenvoudiger wordt. Daarnaast is de opbouw van de norm ook vernieuwend. Met de groei van het aantal managementsysteemnormen, denk alleen al aan ISO 9000 (kwaliteit), ISO 14000 (milieu), OHSAS 18000 (arbo), ISO 22000 (voedselveiligheid), ISO 27000 (informatiebeveiliging), ISO 28000 (supply chain security), ontstond ook het besef dat deze managementsystemen niet naast elkaar moesten bestaan, maar dat de organisatie maar één managementsysteem heeft. Daarop is een kernmanagementsysteem vastgesteld. Op en in dit kernmanagementsysteem moeten de aandachtspunten van de norm worden geïntegreerd. De ISO 22301 is de eerste norm die opgebouwd is volgens dit kernmanagementsysteem. Bij revisies van andere managementsysteemnormen zullen ook die naar deze vorm toegaan. Dit maakt het voor organisaties eenvoudiger om nieuwe aandachtspunten in het managementsysteem 'te pluggen'.

Waar richt ISO 22301 zich op?

BCM richt zich op het kunnen voortzetten van de operationele processen na verstorende incidenten en op het herstel van de bedrijfssituatie. BCM zit in de hoek van de operationele risicobeheersing (zie tabel 1). Daarmee is BCM een vanzelfsprekend instrument voor de operationele manager die verantwoordelijk is voor zijn proces. BCM is echter ook interessant voor een financieel ingestelde risicomanager als bijvoorbeeld de insurance manager. Met het sturen op een BCM-aanpak worden de operationele risico's aangepakt. Met een aantoonbare BCM-aanpak wordt ook op het financiële risico gestuurd en kunnen tevens gunstiger verzekeringspremies worden bedongen.

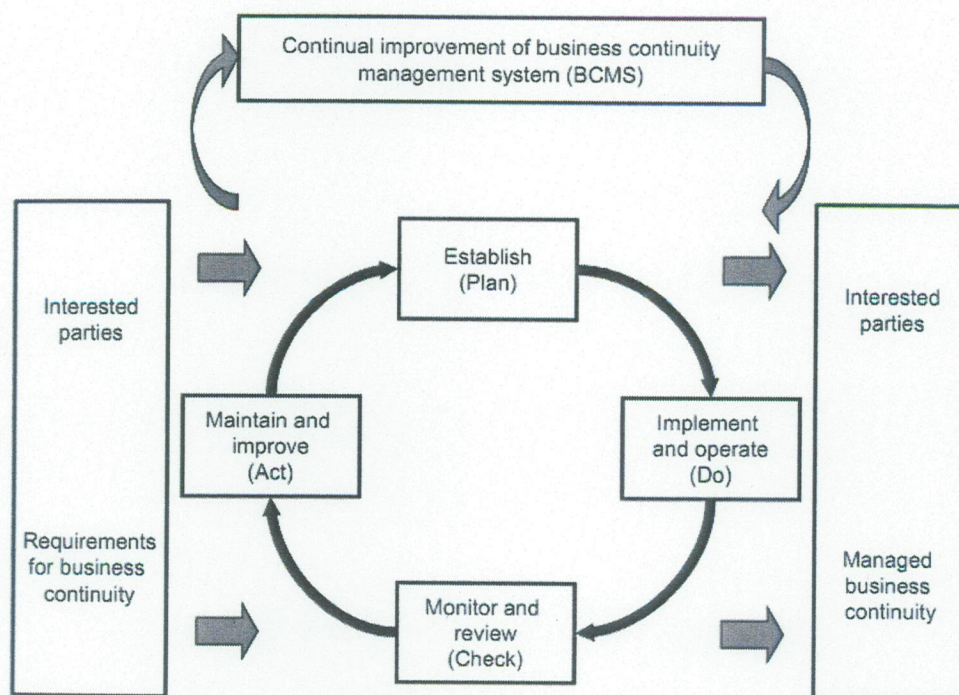
Tabel 1. Risicomanagementaanpak

Operationele risicobeheersing	Risicofinanciering
Vermijden van risico	Delen van risico
• Niet uitvoeren van risicovolle activiteit	• Outsourcing naar klant
	• Outsourcing naar leverancier
	• Outsourcing naar verzekeraar
Verminderen van risico	Retentie
• Verklein kans op incident (preventie)	• Accepteer en budgeteer verlies
• Vergroot redundantie	
• Beperk impact van incident (mitigation)	
• Vergroot herstelcapaciteit	
• Vergroot alternatieve werkwijze	

Wat zijn nu typische incidenten? Denk aan brand, uitval van kritische bedrijfsmiddelen, uitval en corruptie van ICT, uitval van energie, uitval van vervoer, overstromingen en natuurgeweld, uitval van mensen door pandemie en staking, uitval van leveranties. Dit zijn typische incidenten die bij de organisatie weinig voorkomen. Als het incident plaatsvindt, heeft het grote gevolgen. Niet alleen voor

de organisatie zelf, maar ook de processen bij de klanten kunnen hier hinder van ondervinden. De gevolgen zijn niet alleen een directe financiële schade, maar ook een vertrouwensschade. Tot slot zullen door de periode dat de organisatie niet meer kan leveren, klanten andere leveranciers vinden. Uit onderzoek blijkt dat 50 tot 70 procent van organisaties die door een incident worden getroffen en geen bedrijfscontinuïteitsplan (BCP) hebben, niet meer de deuren openen of deze deuren binnen 18 maanden weer sluiten.

De ISO 22301 zelf is een document van ruim twintig pagina's. De norm richt zich op de expliciete of impliciete eisen die stakeholders hebben op de operationele continuïteit van de organisatie en op de wijze waarop deze bedrijfscontinuïteit wordt georganiseerd. De aanpak wordt in een plan-do-check-act-managementaanpak ontwikkeld, uitgevoerd, gecheckt en verbeterd (zie figuur 1).



Figuur 1. PDCA-model voor BCM-processen

Hoe is ISO 22301 te gebruiken?

Puntsgewijs weergegeven is de ISO-aanpak als volgt toe te passen:

- Allereerst kan de aanpak worden gebruikt als hulpmiddel om de organisatie van de continuïteit te checken en te zien waar verbeteringen mogelijk zijn.
- Daarnaast kan de aanpak worden gebruikt om daadwerkelijk een managementsysteem in te voeren voor de verbetering van de continuïteit en het risicomanagement van de eigen organisatie. Risico's worden doordachter genomen, waardoor de organisatie bepaalde risico's uit de weg kan gaan of juist bewuster kan nemen. Veel risico's kennen immers zowel positieve als negatieve aspecten.
- Met toepassing van deze norm beschikt de organisatie over operationele procedures om bij een incident de belangrijkste processen voort te kunnen zetten en tot herstel van

de oude situatie over te gaan. Dit wordt het bedrijfscontinuïteitsplan (BCP) genoemd. Natuurlijk dient dit plan wel regelmatig geoefend te worden.

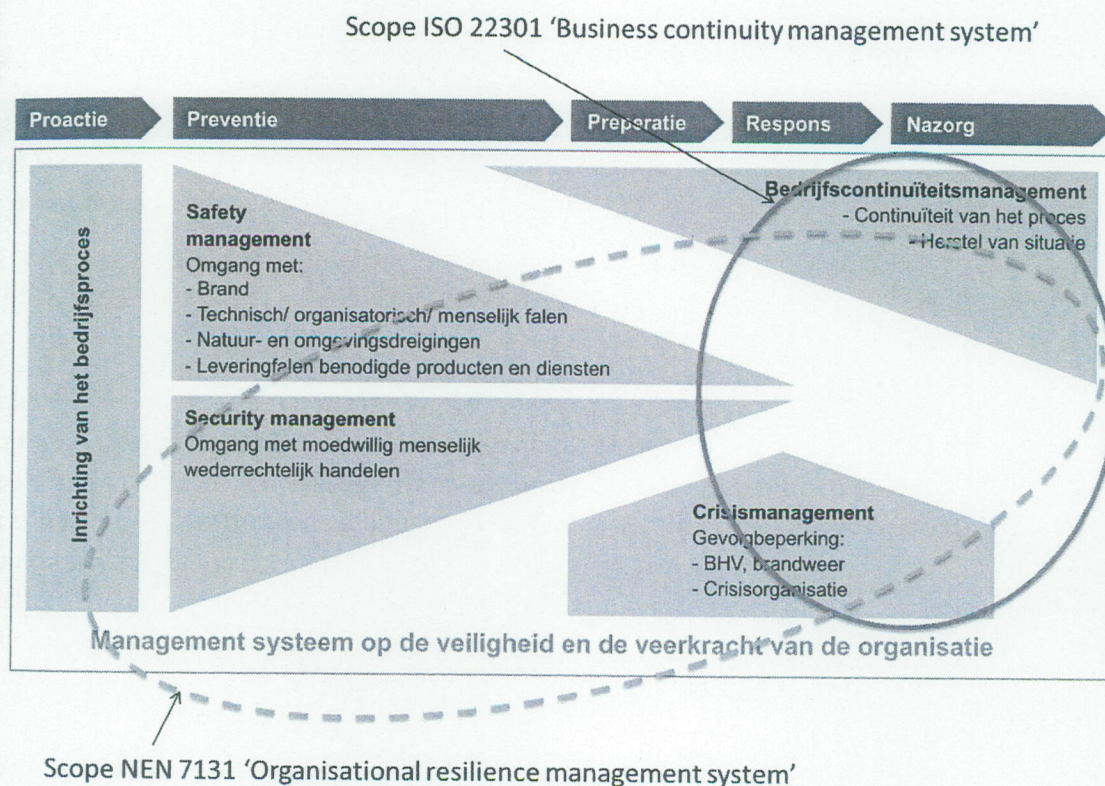
- De norm kan geïntegreerd worden met een organisatiebrede aanpak op het gebied van risicomanagement, bijvoorbeeld de ISO 31000. Maar dit kan ook een andere aanpak voor enterprise risk management zijn, bijvoorbeeld COSO. Beide aanpakken sturen op organisatiebrede risico's. Een van de risicobeperkende maatregelen hierin is BCM.
- Met het toepassen van de norm ontstaat in de organisatie veel kennis op afhankelijkheden, mogelijke verstoringen en op aanpakken bij verstoringen. Deze kennis werpt ook zijn vruchten af voor andere kwaliteitsverbeteringen.
- De stakeholderanalyse is elementair om goed te communiceren op verwachtingen en beleid tijdens de 'koude fase' en op effectieve aanpak rond de verstoring zelf, de 'warme fase'. Hierdoor kan gericht op stakeholderwaardering en beperking van reputatieschade gestuurd worden.
- Een managementsysteem ondersteunt tevens een efficiënt beheer van de plannen. Zonder managementsysteem zijn plannen snel verouderd en is het onduidelijk of de kennis op deze plannen nog in de hoofden van betrokkenen zit. Daarnaast is het efficiënter om één managementsysteem te hebben in plaats van voor alle compliance-eisen verantwoordingsprocessen in te richten.
- Een BCM-aanpak kan ook commercieel gebruikt worden in de relatie naar klanten. De BCM-aanpak is dan een kwaliteitsstempel, waarmee de organisatie aantoont een betrouwbare leverancier te zijn.
- Een BCM-aanpak verkleint de schadeclaims. De aansprakelijkheidspositie na een incident van een organisatie met een aantoonbare BCM-aanpak is duidelijk anders dan in de situatie waarbij de organisatie op niets was voorbereid.
- Een BCM-aanpak stuurt ook op de continuïteit en kwaliteit van leveranciers en subcontractors waar de organisatie van afhankelijk is. Door BCM-eisen te stellen krijgt de organisatie enige zekerheid dat de leveranciers operationeel met verstorende incidenten kunnen omgaan.
- Ten slotte kan een BCM-aanpak ook op een hele keten (of branche) worden toegepast. Dit is natuurlijk in de eerste plaats interessant voor toezichthouders en brancheorganisaties om zowel een robuuste keten als een fair level playing field te hebben. Een verbijzondering van ISO 22301 naar een branchenorm ligt dan voor de hand.

Eisen en audit

De gepubliceerde norm bevat eisen (*requirements*). Dit betekent dat organisaties in ieder geval bij zichzelf deze eisen kunnen toetsen en intern en extern duidelijk kunnen maken dat zij hieraan voldoen. Dit wordt de *first party audit* genoemd. Daarnaast zullen naar verwachting veel organisaties deze norm gaan gebruiken om de continuïteit van hun leveranciers te toetsen. Dit zijn dan leveranciersaudits ofwel *second party audits*. Tot slot ligt het voor de hand dat ook onafhankelijke audit en certificering aangeboden en uitgevoerd zullen worden. Dit is de *third party audit*. Bij de eerste twee type audits bestaat de mogelijkheid om op specifieke bedrijfsaspecten of brancheaspecten te toetsen en bepaalde eisen van de ISO 22301 zwaarder dan wel lichter te wegen; bij de third party audit moet aan alle eisen van de norm worden voldaan. Naar verwachting zal ISO eind 2012 een guideline op de ISO 22301 publiceren. Deze is bedoeld om meer handen en voeten te geven aan de implementatie en het gebruik van de aanpak.

ISO 22301 versus NEN 7131 'Organisational resilience management system'

We kennen ook de NEN 7131 'Organisational resilience management system'. Ook deze richt zich op kritieke bedrijfsmiddelen en processen en in deze norm worden plannen vastgelegd wat de organisatie kan doen voor, tijdens en na een verstorend incident. Het bereik van NEN 7131 is breder dan die van de ISO 22301 en deze norm kan bruikbaar zijn in organisaties waar de plannen op preventie, crisisbeheersing en continuïteitsmanagement in eenzelfde groep worden beheerd. Naar verwachting zal ook deze NEN 7131 naar een ISO-norm toe gaan, maar mogelijk zal dit dan in de vorm van een 'guideline' zijn en geen 'requirements'-document.



Figuur 2. Scope ISO 22301 versus NEN 7131

Tot slot

Uitval van primaire processen of kritieke bedrijfsmiddelen hindert niet alleen de eigen organisatie, maar kan ook gevolgen hebben voor klanten en andere belanghebbenden. Indien uitval te lang duurt, vinden klanten alternatieve leveranciers en is de organisatie 'out of business'. Voor veel organisaties wordt BCM een steeds belangrijker instrument om op risico's te kunnen sturen en om de plannen aantoonbaar gericht en actueel te houden. BCM heeft ook commerciële waarde als 'kwaliteitsstempel'. Door de universele aanpak en het internationale draagvlak is ISO 22301 een goede basis om het managementsysteem voor operationele bedrijfscontinuïteit mee in te richten.