Gaat de nieuwe norm ISO 22301 Business Continuity Management op de Nederlandse agenda's krijgen?

Belangstelling voor BCM groeit na publicatie van ISO 22301:2012

Sinds november 2007 was BS 25999-2:2007 de enige certificeerbare norm voor Business Continuity Management (BCM). Dit heeft tot op heden niet geleid tot een stormloop bij de certificerende instanties. Slechts enkele organisaties zijn overgegaan tot certificering. Na publicatie van ISO 22301:2012 (Societal security – Business Continuity Management Systems – Requirements) op 15 mei jl. is daar verandering in gekomen. Er is duidelijk veel meer belangstelling voor BCM en organisaties realiseren zich, zeker in deze economisch instabiele periode, dat dit onderwerp meer aandacht verdient.

Door Gert Kogenhop

De norm van het British Standards Institution (BSI) is per 1 november jl. ingetrokken ten faveure van de in 163 landen geaccepteerde ISO norm. Tot die datum was het mogelijk de certificering conform BS 25999 af te ronden. Voor gecertificeerde organisaties kan een soepele overgang naar de ISO norm worden bewerkstelligd in samenwerking met bijvoorbeeld BSI tot medio 2014. De algemene verwachting is dat de wereldwijde acceptatie van ISO-normen zal leiden tot een gestage groei van organisaties die hiermee aan de slag gaan — of wellicht onder druk, moeten. Die druk kan komen van onder andere klanten (bijvoorbeeld naar aanleiding van de uitkomst van een ISAE 3402), overheidsbemoeienis (bijvoorbeeld DNB, mei 2011 – Toetsingskader Business Continuity Management Financiele Kerninfrastructuur), aandeelhouders of investeerders en moeder- of zusterorganisaties in landen waar de wetgeving op dit gebied verder gaat dan hier, bijvoorbeeld in het Verenigd Koninkrijk.

Wat is BCM volgens ISO 22301?

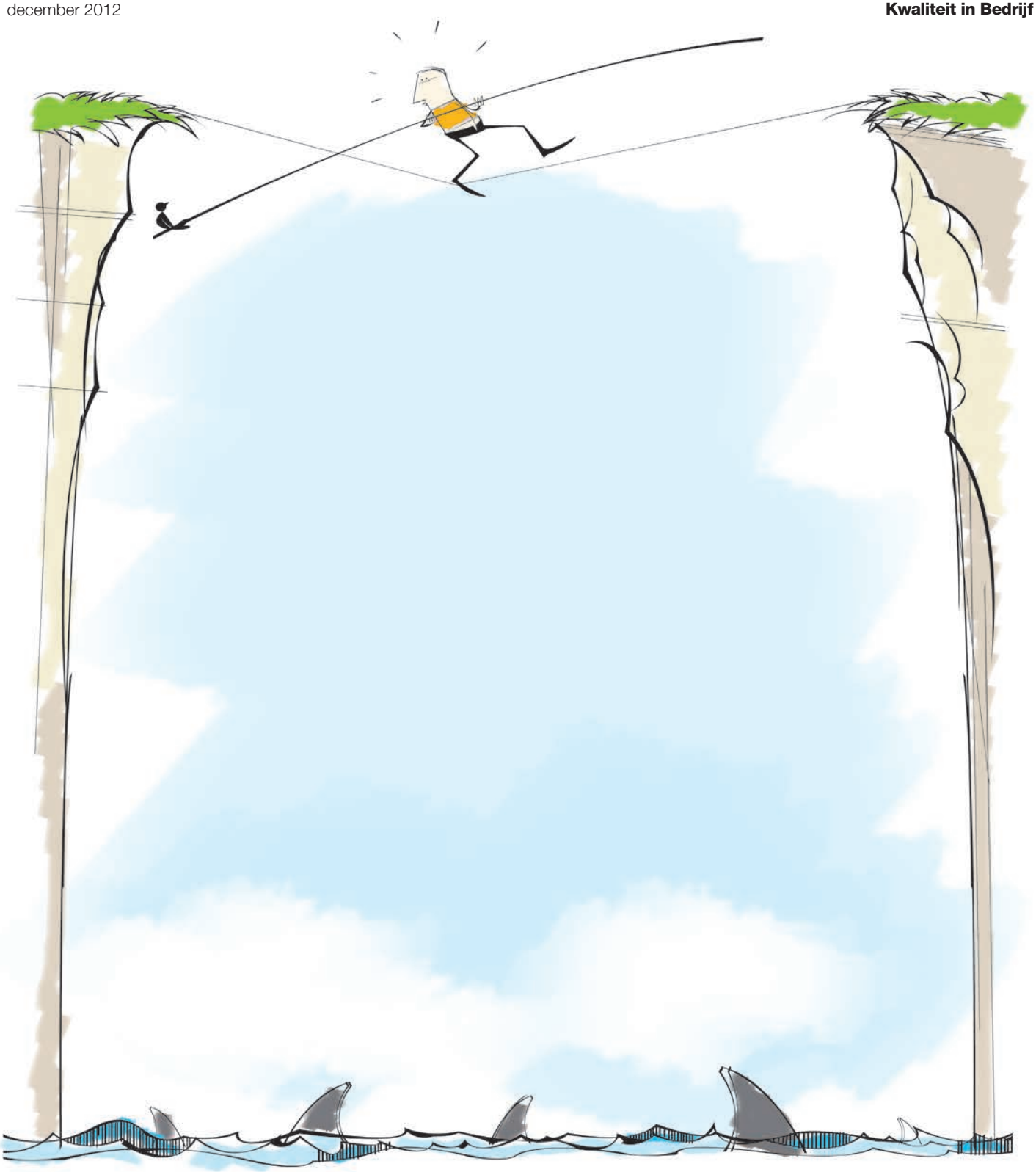
De definitie wijkt niet substantieel af van de Britse versie die tot op de dag van vandaag werd gebruikt en wordt hierin omschreven als: 'Holistisch managementproces dat potentiële gevaren voor een organisatie identificeert en tot welke gevolgen deze gevaren mogelijk kunnen leiden met betrekking tot de operationele activiteiten. Het schept een kader voor het opbouwen van organisatorische weerstand en veerkracht, leidend tot een effectieve reactie welke de belangen van betrokkenen, reputatie, merk en waarde creërende activiteiten veiligstelt'. Met holistisch wordt in dit kader het geheel en de onderlinge samenhang bedoeld, van zowel de organisatie zelf als de directe omgeving, zowel fysiek als de (logistieke en organisatorische) keten met afhankelijkheden.

'Voorbereiding is 90% van het resultaat'

Is ISO 22301 anders dan BS 25999?

Business Continuity Management volgens ISO 22301 heeft dezelfde lading als binnen BS 25999. Enkele definities van gebruikte termen zijn toegevoegd of gewijzigd, terwijl ook enkele zijn verdwenen. Dit laatste omdat deze niet worden toegepast in de ISO-norm of omdat de invulling wordt vrij gelaten. Op zich een goede ontwikkeling, zeker als het gaat om de vrije invulling. Voor de certificerende instanties zullen de verschillen in invulling wellicht kunnen leiden tot interpretatieverschillen, maar die zijn onvermijdbaar. Zaken als het beleidsplan, de feitelijke continuïteitsplannen, de Bedrijfs Impact Analyse (BIA) en Risico Beoordeling (RB), de reactiestructuur en organisatie van het controleren, beoordelen, herzien, onderhouden en continu verbeteren van het managementsysteem zijn enigszins aangescherpt en veranderd op detailniveau, maar leiden zeker niet tot substantiële veranderingen en inspanningen tijdens een eventuele conversie. Laten we concluderen dat als gevolg van opgedane ervaring met de norm BS 25999 en voortschrijdend inzicht, de specialisten hebben gemeend dat de nu vastgelegde elementen leiden tot een beter Business Continuity Management System (BCMS).

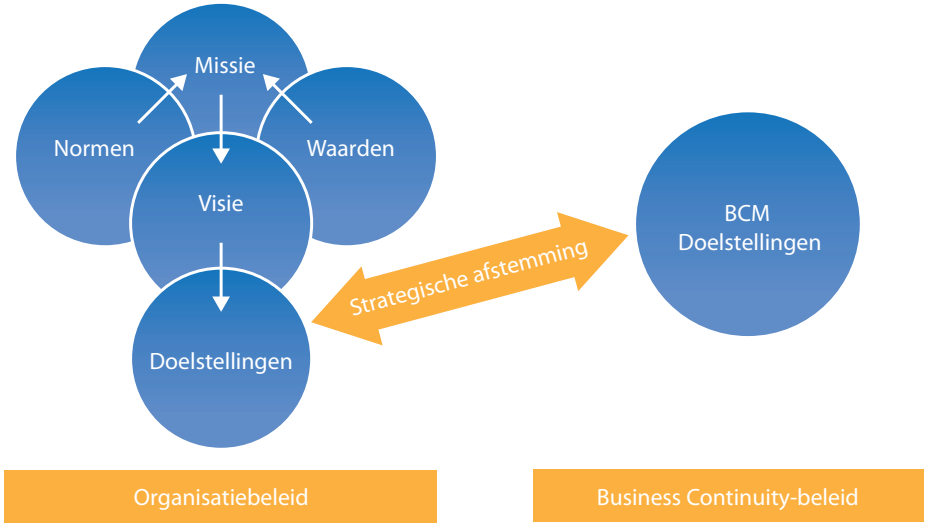
De structuur van ISO 22301 is wezenlijk anders dan die van de BS 25999. Het zesstappenplan is niet meer terug te vinden, de Plan-Do-Check-Act (PDCA)-cyclus echter wel. De zes stappen binnen BS 25999 bestonden elk weer uit een aantal activiteiten, leidend tot, laten we het noemen, zo'n 15 elementen. Binnen de ISO-norm zijn deze allemaal terug te vinden en wordt de implementatie en het beheer aangepakt in 17 stappen — of elementen, zo u wilt. De grootste wijzigingen zijn vooral terug te



vinden op de volgende gebieden:
- systeembeheer (management);
- betrokkenheid van het bestuur van de organisatie (top management); en
- communicatie voor, tijdens en na een ernstig incident (disruptive incident).

ISO werkt momenteel volgens een nieuwe structuur en maakt gebruik van standaardteksten die geschikt zijn voor alle ISO-normen. Op deze wijze wil men organisaties die meerdere ISO-normen implementeren helpen dit proces te vereenvoudigen. De gebruikte terminologie, definities en de basiselementen van alle managementsystemen worden, voor zover mogelijk, op elkaar afgestemd om doublures en verschillen van opzet en aanpak te voorkomen. Een nobel streven. Deze norm is een van de eerste normen volgens deze werkwijze. De nadruk ligt duidelijk op het vaststellen van de doelstellingen en verwachtingen van het BCMS en het meten en controleren van de prestaties; de voortgang en de gerealiseerde resultaten nemen een veel belangrijker positie in. Meer aandacht wordt geschonken aan de planning en voorbereiding van de benodigde inzet van mensen en middelen, voor het zo optimaal mogelijk waarborgen van de bedrijfscontinuïteit.

Meer dan voorheen geldt: ‘Voorbereiding is 90% van het resultaat’. Het feit dat de bestuurders van de organisatie volledig betrokken dienen te zijn bij het begrijpen en vaststellen van de vereisten (benodigdheden), het bepalen van de doelstellingen en het meten van de resultaten, zal zeker leiden tot eerdere en betere acceptatie van



Figuur 1: De strategische afstemming binnen ISO 22301.

BCM als wezenlijk onderdeel van 'Good Governance'; maatschappelijk verantwoord ondernemen (MVO). Tegelijkertijd moet men zich echter realiseren dat de vereiste actieve betrokkenheid van de bestuurders tevens de achilleshiel kan zijn. De praktijk is anders dan de gewenste situatie, de ideale invulling op — uiterst geduldig — papier.

De inhoud en aanpak conform ISO 22301

Plan

Conform de PDCA-cyclus wordt gestart met de Plan-fase (vaststellen). In deze fase wordt allereerst aandacht besteed aan de 'context van de organisatie'. In deze fase worden zaken vastgelegd met betrekking tot onder andere de activiteiten van de organisatie, functies, producten, diensten, samenwerkingsverbanden, logistieke keten en de relaties met belanghebbenden. Dit alles in relatie tot de mogelijke gevolgen van een ernstig incident. In de internationale norm wordt overigens nu gesproken over 'interested parties' en niet meer over 'stakeholders'. Voorts dient er in het beleidsplan een volledige afstemming te zijn met de missie, visie en doelstellingen van de organisatie (zie figuur 1) en het gewenste risicoprofiel (risk appetite). Tevens dient er rekening te worden gehouden met de behoefte en verwachtingen van de relevante (externe) belanghebbenden en de eventueel van toepassingzijnde wet- en regelgeving.

Zoals al eerder aangegeven wordt de nadruk duidelijk gelegd op de betrokkenheid en inzet (het commitment) van de bestuurders van de organisatie. Binnen het onderdeel 'Leiderschap' wordt hier vorm aan gegeven middels het verantwoordelijk stellen van de bestuurders voor onder andere het:

- vaststellen van het beleidsplan;
- zorgdragen voor het linken van het BCMS aan de strategische richting;
- integreren van het BCMS in alle processen;
- beschikbaar stellen van de benodigde mensen en middelen;
- vaststellen van de rollen, verantwoordelijkheden en bevoegdheden van betrokkenen;
- sturen en ondersteunen van continue verbeteringsinitiatieven; en
- communiceren van voortgang en resultaat.

De bestuurders dienen aldus de strategische doelstellingen van het BCMS vast te stellen, alsmede de grondbeginselen. Deze bestaan uit het definiëren van de minimale prestatieniveaus met betrekking tot het leveren van producten en/of diensten en bedrijfsactiviteiten, op een dusdanig niveau dat het behalen van de doelstellingen van de organisatie wordt gegarandeerd. Dit alles dient meetbaar te zijn, rekening houdend met betrokken belanghebbenden, en gecontroleerd en bijgestuurd te worden.

Hier ligt aldus een enorme (terechte) druk bij de bestuurders van de organisatie.

Als laatste onderdeel binnen de Plan-fase dienen zaken te worden vastgelegd met betrekking tot de uitvoering en ondersteuning. Het gaat hier om de dagelijkse gang van zaken; het zekerstellen dat de juiste, gekwalificeerde mensen en middelen voor elke taak worden ingezet. Voorts de juiste ondersteuning, eventueel in de vorm van kennis en vaardigheden van buiten de organisatie; specialisten. Het is van het grootste belang dat iedereen binnen de organisatie beseft wat het belang is van een goed functionerend BCMS en dat men zich bewust is van mogelijke gevolgen bij niet, onvoldoende of zelfs verkeerd reageren (awareness). Belangrijk is zeker in dit geval de communicatie aangaande in eerste instantie het implementatieproces en vervolgens het beheren van het BCMS. Dit alles als vanzelfsprekend ondersteund door een informatiesysteem (document management system), dat een waterdichte 'audit trail' garandeert.

Do

De executie van het BCMS is de Do-fase (implementeren en uitvoeren). Dit bevat onder andere de vaststelling van:

- de Bedrijfs Impact Analyse (BIA);
- de Risico Beoordeling (RB);
- de Business Continuity Strategie;
- de Business Continuity Procedures (BCP); en
- test- en Oefenprocessen.

Het is van het grootste belang dat continu wordt beoordeeld of de activiteiten in dit kader in lijn liggen met de algemene richting waarin de organisatie zich beweegt. Met inbegrip van de wensen en eisen van belanghebbenden, inclusief eventueel van toepassing zijnde wet- en regelgeving. Bij het bepalen van de strategie is het een voorwaarde te kiezen voor haalbare oplossingen, ook al klinkt dat zo logisch en vanzelfsprekend. Afstemming binnen de

'ISO 22301 zal bijdragen aan de acceptatie van BCM als waardevol managementinstrument'

organisatie, de mensen op de werkvloer, is van doorslaggevend belang bij het implementeren van een (mogelijk/hopelijk) succesvol BCMS. Er dienen prioriteiten te worden gesteld in deze fase en aldus keuzes gemaakt te worden over de beschikbaarheid van zaken als mensen, werkplekken, informatie (data), machines en materialen, alsmede zakenpartners, leveranciers en klanten. Dit is uiteindelijk terug te vinden in de te kiezen reactiestructuur, waarin regelingen en afspraken worden opgenomen aangaande het vaststellen van de gevolgen (impact) en daaraan gekoppelde respons. Dit kan zijn: het in werking stellen van de initiële actie/reactie-handelingen, coördineren en communiceren, herstel en/of mogelijk activeren van alternatieve werkwijzen of uitwijk. Het communicatieplan, zowel intern als extern, dient robuust en flexibel te zijn. De tijdigheid en wijze waarop wordt gecommuniceerd is van doorslaggevend belang bij de uitvoering van het actieplan. Voorbeelden te over, helaas, waar dat in het (nabije) verleden vreselijk mis is gegaan. Het is dan ook goed vast te stellen dat de norm hier op adequate wijze aandacht voor vraagt.

Check

In de Check-fase (controleren en beoordelen) ligt de nadruk op het evalueren van de prestatie/uitvoering. In de norm is opgenomen dat er continue controle dient plaats te vinden op het BCMS alsook op periodieke beoordeling en herziening ter verbetering. Controle is vereist op onder andere het behalen van de doelstellingen, het meten van de prestaties (processen, procedures en werking) en het voldoen aan hetgeen gesteld in de norm. Voorts dient de organisatie resultaten te analyseren en na evaluatie van de uitkomsten, verbeter- en correctieve acties te initiëren (audit trail).
Als vanzelfsprekend is een interne auditprocedure een vaststaand onderdeel van de vereisten. Deze dient gericht te zijn op zowel de interne doelstellingen als de vereisten gesteld in deze internationale norm.

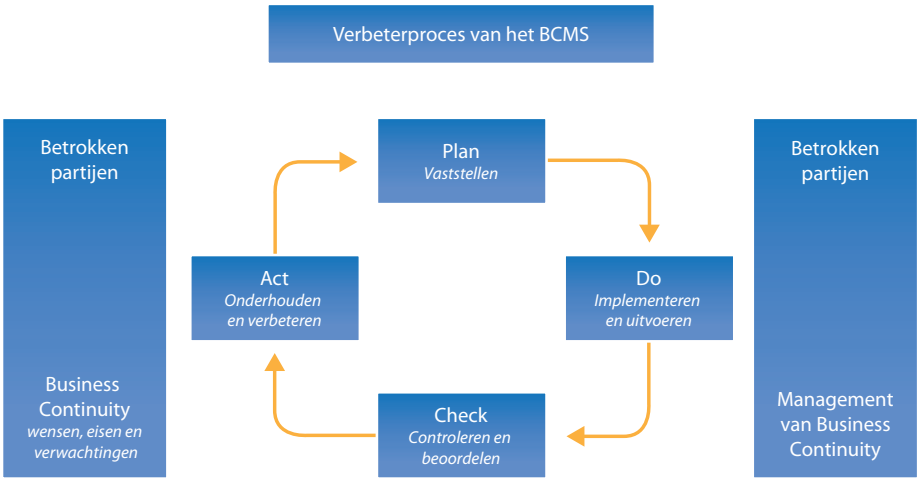
Een van de grootste verschillen met BS 25999 komt tot uiting als we kijken naar de periodieke beoordeling door de bestuurders (management review). In de ISO-norm is deze meer gedetailleerd als het gaat om de vereisten. Duidelijk is wederom de focus op betrokkenheid en inzet (commitment) van de bestuurders. Het proces dient dan ook zeer serieus genomen te worden en niet als sluitpost op de agenda te komen. De uitkomst van deze beoordeling is de input voor de laatste fase.

Act

In de Act-fase (onderhouden en verbeteren) dient elke afwijking (nonconformity) met een actieplan te worden beloond. Na vaststelling van de afwijking dienen correctieve maatregelen te worden genomen en moeten deze strikt worden (op)gevolgd. Het onderhoud en herzien van alle onderdelen van het BCMS behoort zeker ook te worden meegenomen in deze fase. Een continu verbeterproces is een vereiste, waar ook de bestuurders van de organisatie niet te licht over moeten denken. Het gaat in dit geval om activiteiten in de organisatie die een bijdrage leveren aan de effectiviteit (het behalen van de doelstellingen) en efficiency (een optimale mix van kosten en baten) van veiligheidprocessen en procesbeheersing, met als doel een hoger rendement voor de organisatie en haar belanghebbenden. Al met al is deze fase vooral gericht om te leren van het heden en het verleden om beter voorbereid de (onzekere) toekomst tegemoet te kunnen treden. Regeren is vooruitzien!

Een positieve bijdrage

Een van de belangrijkste onderdelen van de taak van bestuurders van organisaties is het ‘zo optimaal mogelijk waarborgen van de bedrijfscontinuïteit’. In de praktijk blijkt telkens weer dat er steken vallen, zoals recentelijk diverse malen in onder andere ziekenhuizen, bij chemiebedrijven, overheidsinstellingen, banken en telecombedrijven. ISO 22301 is een norm die mensen aanspreekt op bovenstaande verantwoordelijkheid en waarin een kader wordt geschept om invulling te geven aan deze noodzaak. Het moet (hoger) op de agenda’s in de bestuurskamers komen. Iedere organisatie wil er morgen toch ook nog zijn? Feit is dat de internationale acceptatie van een certificeerbare norm zeker een positieve bijdrage levert aan de acceptatie van Business Continuity Management als waardevol managementinstrument op zich. *Q*



PDCA ISO 22301.

Over de auteur

Gert Kogenhop is directeur van bcm+, een bedrijf dat is gespecialiseerd in advies en implementatiebegeleiding van Business Continuity Management Systemen conform de norm BS 25999 en ISO 22301. Dit gebeurt in samenwerking met KWA Bedrijfsadviseurs. Tevens worden in samenwerking met de Business Continuity Academy diverse trainingsprogramma’s verzorgd op dit gebied. Voor meer informatie kunt U terecht op www.bcmplus.nl of per e-mail: gk@bcmplus.nl.