



Evaluatie van de BCMS-prestaties

In elke ISO-norm die conform de High Level Structure (nieuwe term sinds mei 2021: Harmonized Structure) is samengesteld, vormt hoofdstuk 9 een belangrijk onderdeel. Hierin worden de procedures voor het monitoren, meten, analyseren en evalueren van de prestaties en doeltreffendheid van het managementsysteem voor bedrijfscontinuïteit of Business Continuity Management System (BCMS) beschreven. Ook de interne audit en de management review komen hier ter sprake.

Door Gert Kogenhop, bcm+

Zoals geldt voor elk managementsysteem zijn de kwaliteit en effectiviteit afhankelijk van hoe volledig, actueel en correct de inhoud is. Dit onderhoud wordt beschreven in hoofdstuk 8.6., als onderdeel van de uitvoering. De organisatie behoort haar bedrijfsimpactanalyse, risicobeoordeling, strategieën en oplossingen, bedrijfscontinuïteitsplannen en -procedures te evalueren om de (continue) geschiktheid, toereikendheid en doeltreffendheid ervan te bewerkstelligen. Evaluatie van de BCMS-prestaties wordt beschreven in een apart hoofdstuk. Belangrijke onderdelen voor het monitoren, meten, analyseren en evalueren zijn: het vaststellen van de methoden die hiervoor benodigd zijn, het onderzoeken van historisch bewijs, in welke mate het beleid en de doelstellingen gehaald worden en of de van toepassing zijnde wet- en regelgeving wordt nageleefd. Afwijkingen en tekortkomingen worden gemonitord en acties dienen te worden geïnitieerd om deze te corrigeren. Een lastig onderdeel voor elke organisatie blijft

het bepalen van de prestatie- of risico-indicatoren. Meten hoe succesvol de organisatie is in het beperken van de uitvaltijd bij een ernstig incident, doelstellingen aangaande bijvoorbeeld de veiligheidsvoorraad en mogelijke alternatieven bij supply chain verstoringen of het effectief zijn van uitwijklocaties en thuiswerken. Vaak wordt gewerkt met het meten van het aantal geplande interne audits, oefeningen en testen, naast wellicht het stellen van doelstellingen op het gebied van mitigerende maatregelen gericht op risicoverkleining, kans op en impact van incidenten.

De management review

De interne auditfunctie is voor velen een bekend fenomeen, echter in het geval van BCMS een voor menig een nieuw onderwerp: bedrijfscontinuïteitsbeheer. Grofweg behelst dit het beoordelen of de in het beleidsplan bepaalde doelstellingen gehaald worden, inclusief de juiste werkwijzen rond implementatie en onderhoud en het identificeren van

verbeterkansen. Auditprogramma's worden 'aangevuld' met het onderdeel BCM. Een grote uitdaging is vaak het vinden van competent, onpartijdig en objectief personeel voor de uitvoering (intern of extern ingehuurd).

Het topmanagement is eigenaar van een formeel beoordelingsproces, de management review, met input vanuit diverse onderdelen van het managementsysteem. Allereerst de prestatiemetingen zoals hierboven beschreven, voorts de evaluaties van oefenen en testen alsook van werkelijke activatie van de continuïteitsplannen tijdens een incident. Veranderingen in en buiten de organisatie (bijv. markt-/sector-/branchetrends, supply chain, wet- en regelgeving, acquisities en een reorganisatie) dienen te worden beoordeeld, evenals het beoordelen van mogelijke kansen voor continue verbetering. Een management review behoort te resulteren in verbetering van de doelmatigheid, prestaties en doeltreffendheid van het BCMS. Denk hierbij aan wijzigen van het toepassingsgebied, gekozen strategieën en oplossingen voor bedrijfscontinuïteit, veranderingen in beheersmaatregelen en in het meten van de doeltreffendheid ervan.

Indien de organisatie beschikt over een gecertificeerd BCMS conform ISO 22301, volgt tevens een jaarlijkse externe beoordeling, waarbij de audit wordt uitgevoerd door een certificatie-instelling.

HOE GOED IS UW ORGANISATIE VOORBEREID?

Ook voor mkb-bedrijven geldt: wees voorbereid op risico's en verstoringen. Met MKB zekerheid bouwt u in slechts vier maanden een Plan B voor uw organisatie met behulp van een duidelijk en haalbaar stappenplan.

Meer weten? Download de zelfscan gratis op www.mkbzekerheid.nl



Aandachtspunten voor een BCMS-certificatie-audit

In de Visie 2021-uitgave van Kwaliteit in Bedrijf hebben we een interview geplaatst met Gert Kogenhop. Vorig jaar hebben we om organisaties te helpen zelfs een special rond het thema Business Continuity Management – Plan B magazine – uitgebracht en een bijbehorende website (www.magazineplanb.nl) in het leven geroepen. Steeds meer bedrijven gaan de ISO-norm* op dit gebied toepassen.

met een vooraf vastgestelde capaciteit binnen aanvaardbare tijdsaders te blijven leveren. Er zijn een aantal aspecten waar tijdens de audit op gelet wordt. Deze zijn gericht op het optimaal, structureel kunnen reageren in geval van een verstoring, een incident. Welke structuur zit er in incident response en crisis management? Denk hierbij aan de vastlegging, situatie rapportage (SitRep) en toegepaste

meerdere risico's afdekken? Bij scenario's wordt vaak op verwachte gebeurtenissen gepland, terwijl we toetsen op onverwachte gebeurtenissen. Is de flexibiliteit aanwezig om te kunnen reageren met het gewenste resultaat? Het gaat met name om de operationele incidenten. Welke productieverstoringen worden vastgelegd en hoe wordt hierop geacteerd? Productie betreft meer dan alleen het maken van fietsen of het bakken van brood. Iedereen, banken en verzekeraars, telecomproviders en energieleverancier, de overheid, heeft producten en diensten, en dus productieafdelingen.'



Wanneer besloten wordt dit management-systeem te laten certificeren door een certificatie-instelling, leidt dit onvermijdelijk tot een bezoek – van enkele dagen – door een externe auditor.

In deze bijdrage hebben we (KiB) een interview met adviseur en ISO 22301 auditor Jan van Buiten (JvB) en kregen we een antwoord op de vraag: 'Waar moet de organisatie tijdens een audit op letten?'

JvB: 'Ik wil dit graag pareren met de hoofdvraag voor deze audit: "Is de organisatie in staat om gestructureerd te reageren op onverwachte gebeurtenissen?" Dat is het uiteindelijke doel van business continuity. Toetsen van het vermogen van een organisatie om tijdens een verstoring producten en diensten

methodiek, zoals BOBOC (Beeldvorming, Opties, Besluit, Opdracht en Controle). Voorts is het beoordelen of er wordt gestuurd op de kritische activiteiten voor het leveren van producten/diensten een belangrijk aspect. Iets wat helaas vaak ontbreekt in de analysefase.

En ten slotte hoe de evaluatie van het incident response proces is geborgd: het leren van incidenten.'

KiB: Je kunt onmogelijk alles voorzien, dus we begrijpen de focus op een gestructureerde reactie. Hoe kun je je voorbereiden op dingen die je niet kunt voorzien?

JvB: 'Als auditor kijk ik vooral naar onverwachte gebeurtenissen. Hoe zijn de business continuity plannen (BCP's) opgezet? Is dit risicogericht of voor verschillende scenario's die

KiB: Zijn er nog organisatorische aspecten waar speciaal op gelet wordt?

JvB: 'In het geval van een ernstige verstoring is het Crisis Management Team (CMT) de spil, de spin in het web. De Business Continuity Management Teams (BCMT's) en in geval van bijvoorbeeld een cyberincident het Cyber Security Incident Response Team (CSIRT) en in geval van een ontruiming het BHV Team, moeten tezamen de optimale reactiestructuur vormen. Hoe is dit ingericht en geborgd? Regelmatig zie ik dat alleen topmanagement een crisistraining krijgt, terwijl tactisch (operationeel) management in de praktijk de meeste incidenten moet oplossen.'

KiB: Verder nog aandachtspunten?

JvB: 'Ik kijk zeker ook naar de context van kwetsbaarheden, bedreiging en risico's. Bestaat er afhankelijkheid van externe partijen en wat zijn de karakteristieken van de locatie (kans op brand bij de burens, naast een spoorlijn of water)?'

* *Veiligheid en veerkracht – Managementsystemen voor bedrijfscontinuïteit (business continuity management systems) – Eisen (ISO 22301:2019, IDT).*