ISO 27031 – IT Cybersecurity en Business Continuity

ISO 27031 *'Information technology – Cybersecurity – Information and communication technology readiness for business continuity'* is een redelijk onbekende norm die als het ware een brug slaat tussen IT en BCM. Deze in 2011 gepubliceerde standaard wordt momenteel herzien en verdient extra aandacht nadat deze is gepubliceerd – waarschijnlijk begin 2020.

Het niet beschikbaar zijn van ICT-diensten, inclusief die veroorzaakt worden door het optreden van beveiligingsproblemen, zoals hacking en malware-infecties, heeft invloed op de continuïteit van de bedrijfsvoering. Het beheer van ICT en de gerelateerde continuïteit en andere beveiligingsaspecten vormen aldus een belangrijk onderdeel van de vereisten voor bedrijfscontinuïteit. Bovendien zijn de geprioriteerde, kritische activiteiten die bedrijfscontinuïteit vereisen nagenoeg altijd (volledig) afhankelijk van ICT. Deze afhankelijkheid betekent dat verstoringen van ICT strategische risico's kunnen vormen voor de reputatie van de organisatie en haar vermogen om producten en diensten te leveren. 'ICT-readiness' is een essentieel onderdeel voor veel organisaties bij de implementatie van bedrijfscontinuïteitsbeheer en informatiebeveiligingsbeheer. Als onderdeel van de implementatie en werking van een informatiebeveiligingsbeheersysteem (ISMS) zoals gespecificeerd in respectievelijk ISO 27001 en het bedrijfscontinuïteitsbeheersysteem (BCMS) in ISO 22301, is het van cruciaal belang om een plan voor de ICT-diensten te ontwikkelen en te implementeren om de organisatie te helpen de continuïteit te verzekeren.

Deze standaard verdient meer aandacht en toepassing, omdat we *onverantwoord* afhankelijk zijn van ICT.

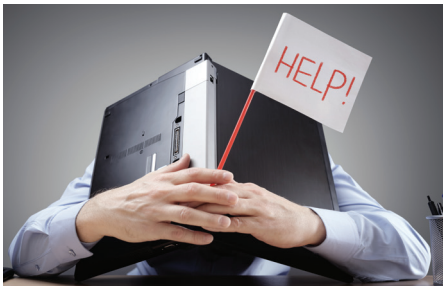
Hoe afhankelijk is uw organisatie van ICT?

Stel uzelf eens de vraag: 'Kan ik zonder ICT en dan misschien iets specifieker, zonder bepaalde applicaties, mijn werk doen?' In heel veel organisaties is dan het antwoord iets in de richting van 'Nee' of 'Nou.... daar vraag je me wat, ik denk dat dat niet eenvoudig wordt'. Naast de broodnodige mailapplicaties om met elkaar te communiceren (vaak Outlook) en Microsoft Office 365, met onder meer Word, Excel en PowerPoint waar we dagelijks mee werken, zijn er doorgaans tientallen applicaties die we in onze processen gebruiken. Als daar een probleem mee is, ze doen 't niet, dan wijzen we naar de ICT-afdeling die het maar moet oplossen. Maar wat doet ú als proceseigenaar en dus verantwoordelijke in zo'n situatie?

Door Gert Kogenhop, bcm+

Het is duidelijk dat de afhankelijkheid van ICT enorm is en alleen nog maar verder gaat toenemen. Eigenlijk een onaanvaardbare afhankelijkheid, waar we van wegkijken of het gemakshalve negeren of zelfs ontkennen. ICT Continuity of indien er een 'probleem' is Disaster Recovery is dan ook steeds belangrijker. Er wordt veel tijd, geld en energie gestoken in redundancy, zoals het werken met meerdere datacenters en allerlei oplossingen om te voorkomen dat ICT-onderdelen – waaronder informatiebeveiliging – uitvallen. Duidelijk gesteld dient te worden dat ICT Continuity (het zorgdragen voor continuïteit van de ICT en een foutloze implementatie van het Disaster Recovery plan als er toch iets gebeurt) iets anders is dan Business Continuity. Dit is het zorgdragen dat we onze producten en diensten kunnen blijven leveren, wat er ook gebeurt. Hierbij is ICT-uitval één van de bedreigingen, naast bijvoorbeeld brand, personeelstekorten door een OV-staking of het stilvallen van een productielijn door een storing of problemen

in de supply chain, als gevolg van extreem winterweer.
Eén van de belangrijkste elementen tijdens het implementeren van een Business Continuity Management Systeem (BCMS) is het uitvoeren van een risicobeoordeling. Krijgt de afhankelijkheid van ICT en de actuele bedreigingen rond dit thema – denk aan cybercrime – de juiste aandacht en het benodigde gewicht? Goed in ieder geval om in beeld te hebben welke geprioriteerde, kritische activiteiten of processen afhankelijk zijn van bepaalde applicaties of data, bijvoorbeeld om de juiste herstelstrategie paraat te hebben. Kunnen we tóch zonder toegang tot applicaties of data, wellicht tot op zekere hoogte, producten en diensten leveren? En wetende wat we vóóraf kunnen regelen in plannen opnemen, met alternatieven? Wellicht kunnen collega's op andere locaties die werkzaamheden overnemen of kunnen dingen handmatig, of ...
Wat is een acceptabele impact wanneer applicaties uitvallen of data niet beschikbaar is? ICT, waaronder informatiebeveiliging en de herstelstrategie, hangt zeer nauw samen met BCM en de gekozen strategie in geval van een calamiteit. Niet wijzen dus, maar samenwerken, informatie delen en zoveel mogelijk integratie van de werkzaamheden. Zorg voor een plan B, voor zover mogelijk. U laten verrassen en geen idee hebben wat te doen of de handjes in de lucht gooien en beteuterd rondkijken is geen goede herstelstrategie.



Informatiebeveiliging in BCM

Het managementsysteem voor Informatiebeveiliging (IB) is gedefinieerd in de ISO 27001-norm. Naast het managementsysteem, is in deze norm tevens een annex A opgenomen met 114 beheersmaatregelen voor IB. Om tot een adequaat beveiligingsniveau te komen, moeten deze beheersmaatregelen risicogebaseerd geïmplementeerd worden.

Door Johan Bakker CISSP ISSAP CIPM CIPPE CPT, CEO en Founder Unified Vision BV

In de genoemde annex A zit ook een hoofdstukje over BCM. Over dit hoofdstuk ontstaat nogal eens verwarring, wanneer men de ISO 27001 implementeert voor certificering. In de praktijk kom ik menig Security Officer tegen die op basis van de eisen in de annex A een volledig Business Continuity Plan (BCP) opstelt en oefent, gericht op de belangrijkste bedrijfsprocessen. Hoewel dit vanuit bedrijfscontinuïteit bezien misschien wenselijk is, is het voor ISO-27001 certificering echter niet noodzakelijk. Sinds de introductie van de 2013-versie van de ISO 27001, komt deze verwarring al minder voor, omdat de eisen in annex A nu helderder geformuleerd zijn dan in de vorige versie, maar ik zie de discussie toch nog steeds gevoerd worden. Dus wat staat er nu echt in de annex A-eisen in relatie tot BCM?

In annex A beheersmaatregel 17.1.1 staat dat de eisen voor informatiebeveiliging gedurende calamiteiten vastgesteld moeten worden en dat tevens de continuïteit van het IB-beheerproces geborgd moet worden. Wanneer er binnen de organisatie al BCM is ingericht, kunnen deze zaken hieraan toegevoegd worden. Concreet worden er dan eisen in het BCP of in de Disaster Recovery-plannen toegevoegd die de vereiste mate van beschikbaarheid, integriteit en vertrouwelijkheid van bedrijfsinformatie gedurende calamiteiten definiëren. Daarnaast wordt er voor het IB-beheerproces een Business Impact Analyse (BIA) uitgevoerd en worden er zo nodig preventieve en correctieve maatregelen voor de benodigde beschikbaarheid en tijdig herstel van (delen van) dit proces als onderdeel van BCM ingeregeld.

Wanneer er nog geen BCM is ingericht, kan men volstaan met de eis dat bedrijfsinformatie gedurende calamiteiten hetzelfde niveau van beveiliging geniet als in de normale uitvoeringsomstandigheden. Deze eis kan dan bijvoorbeeld onderdeel gemaakt worden van de *incident response plannen*. Wel dient men dan nog de nodige voorzieningen te treffen (en te oefenen) om die eis gedurende *incident response* te kunnen borgen, waarbij eventuele continuïteitsplannen zich kunnen beperken tot de continuïteit of het herstel van het IB-beheerproces zelf. Dat is toch wat overzichtelijker dan de inrichting van full-blown BCM voor de bedrijfsprocessen!