Bijlage 3 – Checklist Interne Audit voor ISO 27001 en ISO 22301

1. Checklist Interne Audit voor ISO 27001

Clausule	Vereisten van de norm	Naleving ja/nee	Bewijs
4.2	Heeft de organisatie belanghebbende partijen bepaald		
4.2	Bestaat de lijst van vereisten alle belanghebbende partijen		
4.3	Is het toepassingsgebied vastgelegd met duidelijk gedefinieerde grenzen en interfaces		
5.1	[illegible]		
5.1	Waarborgt het management dat ISMS zijn doelstellingen realiseert		
5.2	Bestaat het Informatiebeveiligingsbeleid met [illegible] doelstellingen		
5.2	Wordt het Informatiebeveiligingsbeleid gecommuniceerd binnen het bedrijf		
5.3	[illegible] gecommuniceerd		
6.1.2	Is het risicobeoordelingsproces vastgelegd, met inbegrip van het risicoaanvaardingscriteria en het risicobeoordelingscriteria.		
6.1.2, 8.2	Zijn de risico`s geïdentificeerd, hun eigenaren, [illegible]		
6.1.3	In het risicobehandelingsproces vastgelegd, inclusief de risicobehandelingsopties		
6.1.3, 8.3	Zijn alle onacceptabele risico's behandeld [illegible] resultaten vastgelegd		
6.1.3	Wordt de Verklaring van Toepasselijkheid geproduceerd met verantwoording en status van elke beheersmaatregel.		
6.1.3, 8.3	[illegible] aangeleverd door de risico-eigenaren		
6.2	Bepaalt het Plan voor Risicobehandeling wie [illegible] evaluatiemethode is		
7.1	Zijn adequate middelen verstrekt voor alle		

Comment [DK1]: Om te leren hoe je de checklist kan gebruiken:

Webinar "Internal audit: How to conduct it according to ISO 27001 and BS 25999-2" http://www.iso27001standard.com/webinars

Comment [DK2]: Om meer te leren over dit onderwerp, lees dit artikel: How to make an Internal Audit checklist for ISO 27001 / ISO 22301 http://www.iso27001standard.com/blog/2013/11/25/how-to-make-an-internal-audit-checklist-for-iso-27001-iso-22301/

Comment [DK3]: Dit zijn de gestelde eisen van de IOS 27001 norm; u dient zelf uw specifieke eisen in te voegen van uw eigen documentatie.

Comment [DK5]: In te vullen tijdens de audit - Ja of Nee, afhankelijk van de vraag of het bedrijf voldoet of niet.

Comment [DK4]: In te vullen tijdens de audit- opnamen, mondelinge verklaringen of persoonlijke waarnemingen van de auditor die de bevindingen bevestigen.

	onderdelen van het ISMS		
7.2	Zijn alle benodigde vaardigheden gedefinieerd, [illegible] vaardigheden bijgehouden		
7.3	Is het personeel bewust van het [illegible] gevolgen van het niet naleven van de regels		
7.4	Bestaat het proces voor communicatie gerelateerd aan informatiebeveiliging, inclusief de verantwoordelijkheden en wat te communiceren		
7.5	Bestaat het proces voor beheersing van [illegible] ze worden gepubliceerd, opgeslagen en beveiligd		
7.5	Worden alle documenten van externe origine beheerst		
8.1	Worden alle uitbestede processen geïdentificeerd en beheerst		
9.1	Staat gedefinieerd wat er gemeten dient te [illegible] evalueren		
9.1	Zijn de meetresultaten vastgelegd en gerapporteerd aan de verantwoordelijken		
9.2	Bestaat een auditprogramma, wie bepaalt de [illegible] auditcriteria en toepassingsgebied		
9.2	Worden er interne audits uitgevoerd volgens het [illegible] ontstane corrigerende maatregelen		
9.3	Wordt de directiebeoordeling regelmatig uitgevoerd, en worden resultaten vastgelegd in notulen van de vergadering		
9.3	[illegible] belangrijk voor het succes van het ISMS		
10.1	Reageerde de organisatie op elke afwijking		
10.1	Overweegt de organisatie de gevolgen van [illegible] corrigerende maatregelen te nemen		
10.1	Zijn alle afwijkingen vastgelegd, tezamen met de corrigerende maatregelen		
A.5.1.1	[illegible] het management en gepubliceerd		
A.5.1.2	Wordt al het informatiebeveiligingsbeleid [illegible]		
A.6.1.1	Wordt alle informatiebeveiligings-		

	verantwoordelijkheden duidelijk gedefinieerd door een of meerdere documenten		
A.6.1.2	Zijn taken en verantwoordelijkheden gedefinieerd op een dermate manier om conflict van belangen te vermijden, in het bijzonder met de informatie en systemen waar hoge risico's bij betrokken zijn		
A.6.1.3	Wordt duidelijk gedefinieerd wie in contact is met de autoriteiten		
A.6.1.4	Wordt duidelijk gedefinieerd wie in contact dient te zijn met speciale belanghebbende groepen of professionele verenigingen		
A.6.1.5	Zijn er informatiebeveiligingsregels opgenomen in elk project		
A.6.2.1	Zijn er regels voor het veilig behandelen van draagbare apparaten		
A.6.2.2	Zijn er regels bepalend hoe de bedrijfsinformatie wordt beveiligd op telewerken locaties		
A.7.1.1	Worden er achtergrondcontroles uitgevoerd bij kandidaten voor werk of voor aannemers		
A.7.1.2	Vermelden overeenkomsten met werknemers of aannemers de informatiebeveiligings-verantwoordelijkheden		
A.7.2.1	Verlangt het management actief van alle werknemers en aannemers zich te houden aan de informatiebeveiligingsregels		
A.7.2.2	Worden alle relevante werknemers en aannemers getraineed om hun beveiligingstaken uit te voeren en bestaat er een bewustzijnsprogramma		
A.7.2.3	Werden alle werknemers die een beveiligingsinbreuk hebben gepleegd, onderworpen aan een formeel disciplinair proces		
A.7.3.1	Worden informatiebeveiligings-verantwoordelijkheden die geldig blijven na de beëindiging van het dienstverband gedefinieerd in de overeenkomst		
A.8.1.1	Is er een lijst van bedrijfsmiddelen opgesteld		
A.8.1.2	Heeft elk bedrijfsmiddelen een toegewezen eigenaar		
A.8.1.3	Zijn er regels voor dagelijke behandeling van informatie en bedrijfsmiddelen vastgelegd		
A.8.1.4	Leverden alle werknemers en aannemers de bedrijfsmiddelen weer in bij de beëindiging van hun dienstverband		
A.8.2.1	Wordt de informatie geclassificeerd volgens gespecificeerde criteria		
A.8.2.2	Wordt de geclassificeerde informatie gelabled		

	volgens de gedefinieerde procedures		
A.8.2.3	Zijn er procedures welke definiëren hoe om te gaan met geclassificeerde informatie		
A.8.3.1	Zijn er de procedures welke aangeven hoe om te gaan met verwijderbare media in overeenstemming met de classificatieregels		
A.8.3.2	Zijn er formele procedures voor het verwijderen van media		
A.8.3.3	Wordt de media beveiligd tijdens transport welke gevoelige informatie bevat		
A.9.1.1	Bestaat het toegangsbeleid welke bedrijfs- en beveiligingsvereisten voor toegangscontrole definieert		
A.9.1.2	Hebben gebruikers toegang tot alleen die netwerken en diensten voor welke ze specifiek zijn geautoriseerd		
A.9.2.1	Worden toegangsrechten geleverd via een formeel registratieproces		
A.9.2.2	Is er een formeel toegangscontrolesysteem wanneer ingelogd wordt op informatiesystemen		
A.9.2.3	Worden speciale toegangsrechten behandeld met speciale zorg		
A.9.2.4	Worden initiële wachtwoorden en andere geheime authenticatie informatie geleverd op een beveiligde manier		
A.9.2.5	Controleren eigenaren van bedrijfsmiddelen periodiek al de uitgegeven toegangsrechten		
A.9.2.6	Zijn de toegangsrechten van alle werknemers en aannemers verwijderd aan het eind van hun contract		
A.9.3.1	Zijn er duidelijke regels voor gebruiker over hoe wachtwoorden en andere authenticatie informatie te beveiligen		
A.9.4.1	Wordt de toegang tot databases en applicaties beperkt volgens het toegangsbeleid		
A.9.4.2	Wordt er een beveiligd login op systemen geëist volgens het toegangsbeleid		
A.9.4.3	Worden de systemen die wachtwoorden beheren interactief, en maken ze de creatie van veilige wachtwoorden mogelijk		
A.9.4.4	Wordt het gebruik van gebruikerstools, die de beveiligingsmaatregelen van applicaties en systemen kunnen overnemen, streng beheerd en beperkt tot een nauwe cirkel van werknemers		
A.10.1.1	Bestaat het beleid dat encryptie reguleert en bestaan andere cryptografische maatregelen		
A.10.1.2	Worden de cryptografische sleutels degelijk		

	beveiligd		
A.11.1.1	[illegible] informatie beveiligd		
A.11.1.2	Is de entree naar de beveiligde ruimte beveiligd [illegible] geautoriseerde personen toelaat		
A.11.1.3	Worden beveiligde ruimten zodanig gesitueerd dat ze niet zichtbaar zijn voor buitenstaanders, en niet makkelijk te bereiken zijn vanaf de buitenkant		
A11.1.4	[illegible] andere systemen geinstalleerd		
A.1.1.5	Worden de werkprocedures voor beveiligde ruimten bepaald en zijn ze congruent met		
A.11.1.6	Worden laden en los gebieden op een dusdanige [illegible] van het bedrijf kan opkomen		
A.11.2.1	Is de apparatuur op een dusdanige manier gesitueerd dat het beveiligd is voor ongeautoriseerde toegang, en van omgevingsdreigingen		
A.11.2.1	[illegible] stroomtoevoer		
A.11.2.3	Worden de stroom en telecommunicatiekabels beveiligd		
A.11.2.4	Wordt de apparatuur regelmatig onderhouden [illegible] naar goede gebruiken		
A.11.2.5	Wordt de er autorisatie verleend voor informatie en andere bedrijfsmiddelen elke keer dat ze van het bedrijfsterrein worden genomen		
A.11.2.6	Worden de bedrijfsmiddelen afdoende beveiligd [illegible] bedrijfsterrein		
A.11.2.7	Worden al de informatie en in licentie hebbende software van de media of apparatuur met media verwijderd indien worden weggegooid		
A.11.2.8	[illegible] niet in de directe nabijheid ervan zijn		
A.11.2.9	Is er een beleid dat gebruikers dwingt om papieren en media te verwijderen indien ze niet aanwezig zijn, en hun scherm locken		
A.12.1.1	[illegible] vastgelegd		
A.12.1.2	Worden alle wijzigingen aan IT-systemen, maar [illegible] beheerst		

A.12.1.3	Bewaakt iemand het gebruik van middelen en voor het project vereiste capaciteit		
A.12.1.4	[illegible] productieomgeving strikt gescheiden		
A.12.2.1	Is anti-virus software, en andere beveiligingssoftware voor malware geïnstalleerd en ververst		
A.12.3.1	[illegible] back-up uitgevoerd volgens dit beleid		
A.12.4.1	Worden alle gebruikersbestanden, fouten en [illegible] en controleert iemand deze		
A.12.4.2	Worden de logbestanden beveiligd op een dusdanige manier dat onbevoegden deze niet kunnen wijzigen		
A.12.4.3	Worden logbestanden van de administrator [illegible] verwijderen worden ze regelmatig gecontroleerd		
A.12.4.4	Worden de klokken op alleIT-systemen gesynchroniseerd met één enkele bron met de juiste tijd		
A.12.5.1	Wordt de installatie van software streng [illegible]		
A.12.6.1	Gaat iemand over het verzamelen van informatie over kwetsbaarheden, en worden deze kwetsbaarheden snel opgelost		
A.12.7.1	Worden audits van productiesystemen gepland [illegible] het risico voor verstoring minimaliseren		
A.13.1.1	Worden netwerken op een dusdanige wijze beheerst dat zij informatie beveiligen in systemen en applicaties		
A.13.1.2	Worden beveiligingsvereisten het in huis en [illegible] opgenomen in overeenkomsten		
A.13.1.3	Worden groepen van gebruikers, diensten, en systemen gescheiden in verschillende netwerken		
A.13.2.1	Wordt de beveiliging van informatie-overdracht [illegible]		
A.13.2.2	Bestaan overeenkomsten met derde partijen welke de beveiliging van informatie-overdracht reguleert		
A.13.2.3	Worden de berichten die worden uitgewisseld ver het netwerkdeugdelijk beveiligd		
A.13.2.4	Vermeld het bedrijf alle [illegible] opgenomen met derde partijen		

A.14.1.1	Worden de beveiligingsvereisten gedefinieerd voor nieuwe informatiesystemen, of voor enige wijzigingen erop		
A.14.1.2	Wordt de bij de applicatie betrokken via de publieke verzonden informatie afdoende beveiligd		
A.14.1.3	Worden de regel voor beveiligde ontwikkeling van software en systemen gedefinieerd		
A.14.2.1	Bestaan formele wijzigingsbeheersmaatregelen voor het maken van enige wijzigingen naar de nieuwe of bestaande systemen		
A.14.2.3	Worden kritische applicaties getest nadat de operating systems zijn geupdate		
A.14.2.4	Worden alleen de wijzigingen die werkelijk noodzakelijk zijn uitgevoerd op de informatiesystemen		
A.14.2.5	Worden de toepaste bouwprincipes vastgelegd en geïmplementeerd		
A.14.2.6	Wordt de ontwikkelingsomgeving afdoende beveiligd tegen ongeautoriseerde toegang en wijziging		
A.14.2.7	Wordt de uitbestede ontwikkeling van systemen bewaakt		
A.14.2.8	Wordt het testen ongeacht de beveiligingsvereisten zijn geïmplementeerd uitgevoerd tijdens de ontwikkeling		
A.14.2.9	Worden de acceptatiecriteria voor de systemen gedefinieerd		
A.14.3.1	Worden de testgegevens zorgvuldig geselecteerd en beveiligd		
A.15.1.1	Wordt het beleid over hoe de dreiging van risico's gerelateerd aan leveranciers en partners vastgelegd		
A.15.1.2	Worden alle relevante beveiligingsvereisten opgenomen in de overeenkomsten met leveranciers en partners		
A.15.1.3	Bevatten overeenkomsten met cloud providers en andere leveranciers beveiligingsvereisten voor het waarborgen van betrouwbare leveranties van diensten		
A.15.2.1	Worden bij leveranciers regelmatig nagegaan of zij de beveiligingsvereisten nakomen, en go audit indien van toepassing		
A.15.2.2	Wanneer wijzigingen worden gemaakt in overeenkomsten met leveranciers en partners, worden risico's en bestaande processen dan meegenomen		
A.16.1.1	Worden procedures en verantwoordelijkheden		

	voor het beheersen van incidenten duidelijk gedefinieerd		
A.16.1.2	Worden alle informatiebeveiligingsincidenten gerapporteerd op tijdige manier		
A.16.1.3	[illegible] gerapporteerd op beveiligingskwetsbaarheden		
A.16.1.4	Worden alle beveiligingsgebeurtenissen beoordeeld en geclassificeerd		
A.16.1.5	Worden procedures over hoe te reageren op [illegible]		
A.16.1.6	Worden beveiligingsincidenten geanalyseerd om er lering uit te trekken over hoe ze te voorkomen		
A.16.1.7	Bestaan er procedures welke definiëren hoe [illegible] rechtelijk proces		
A.17.1.1	Worden vereisten voor continuïteit van informatiebeveiliging gedefinieerd		
A.17.1.2	Bestaan de procedures die de continuïteit van [illegible] ramp waarborgen		
A.17.1.3	Worden oefeningen en testen uitgevoerd om effectieve response te verzekeren		
A.17.2.1	Is de IT-infrastructuur dubbel uitgevoerd [illegible] de verwachtingen tijdens een crisis te voldoen		
A.18.1.1	Worden alle wet-, regelgeving, contractuele en andere beveiligingsverplichtingen vermeld en vastgelegd		
A.18.1.2	Bestaan procedures dat handhaving van [illegible] het bijzonder gebruikte licenties van software		
A.18.1.3	Worden alle registraties beveiligd volgens de [illegible] vereisten		
A.18.1.4	Wordt persoonlijk te identificeren informatie beveiligd zoals vereist in wetten en regelgeving		
A.18.1.5	Worden cryptografische beheersmaatregelen gebruikt zoals vereist in weten en regelgeving		
A.18.2.1	[illegible] herbeoordeeld door een onafhankelijke auditor		
A.18.2.2	Gaan de managers regelmatig na of [illegible] verantwoordelijkheidsterreinen		
A.18.2.3	Worden informatiesystemen regelmatig [illegible] informatiebeveiligsbeleid en normen		

Checklist Interne Audit voor ISO 22301

Clausule	Vereisten van de norm	Naleving ja/nee	Bewijs
4.2	Heeft de organisatie belanghebbende partijen bepaald		
4.2	Bestaat de lijst van vereisten alle belanghebbende partijen		
4.3	Is het toepassingsgebied vastgelegd definiërend [illegible] worden uitzonderingen verklaard		
5.1	Ondersteunt het management actief de [illegible] bedrijfscontinuïteit		
5.2	Sluit het BCMS aan op de bedrijfsstrategie		
5.2	Laat het topmanagent zien dat het [illegible] communiceren.		
5.2	Is de persoon die verantwoordelijk is voor BCMS benoemd en heeft hij voldoende autoriteit.		
5.2	Bestaat er een bedrijfscontinuïteitbeleid en geeft [illegible] doelstellingen		
5.3	Wordt het bedrijfscontinuïteitsbeleid gecommuniceerd binnen het bedrijf		
5.4	Zijn rollen en verantwoordelijkheden voor [illegible] gecommuniceerd		
6.1	Heeft de organisatie alle risico' s en mogelijkheden geïdentificeerd		
6.1	Heeft de organisatie maatregelen gepland om de risico's en mogelijkheden te adresseren		
6.2	Zijn er doelstellingen gesteld voor de [illegible] naar alle relevante werknemers		
6.2	Zijn de doelstellingen voor bedrijfscontinuïteit meetbaar, worden ze bewaakt en bijgesteld		
6.2	Is gedefinieerd wat er dient te gebeuren om de [illegible] vereist zijn		
7.1	Zijn adequate middelen verstrekt voor alle onderdelen van het BCMS		
7.2	Zijn alle benodigde vaardigheden gedefinieerd, [illegible] vaardigheden bijgehouden		

Comment [DK6]: Dit zijn de gestelde eisen van de IOS 27001 norm; u dient zelf uw specifieke eisen in te voegen van uw eigen documentatie.

Comment [DK8]: In te vullen tijdens de audit - Ja of Nee, afhankelijk van de vraag of het bedrijf voldoet of niet.

Comment [DK7]: In te vullen tijdens de audit- opnamen, mondelinge verklaringen of persoonlijke waarnemingen van de auditor die de bevindingen bevestigen.

7.3	Is het personeel bewust van het bedrijfscontinuïteitbeleid, van hun rol, en de gevolgen van het niet naleven van de regels		
7.4	Bestaat de procedures welke bepalen wat te communiceren gerelateerd aan bedrijfscontinuïteit, wanneer het te communiceren, en aan wie		
7.5	Bestaat het proces voor beheersing van documenten en registraties, inclusief wie de documenten nakijkt en goedkeurt, waar en hoe ze worden gepubliceerd, opgeslagen en beveiligd		
7.5	Worden alle documenten van externe origine beheerst		
8.1	Worden alle uitbestede processen geïdentificeerd en beheerst		
8.2.1	Zijn de processen voor Risicobeoordeling en business impact analyse gedefinieerd en vastgelegd		
8.2.2	Worden business impact analyses uitgevoerd, inclusief alle activiteiten, en wordt de impact van het niet uitvoeren van deze activiteiten in de tijd beoordeeld		
8.2.2	Is er voor iedere activiteit een maximaal toelaatbare uitvalduur bepaald en zijn de onderlinge afhankelijkheden geïdentificeerd		
8.2.3	Is van alle activiteiten, processen en bedrijfsmiddelen een risicobeoordeling gemaakt en zijn verstoringen die moeten worden aangepakt geïdentificeerd		
8.3.1	Zijn voor alle activiteiten hersteltijden (RTO) bepaald		
8.3.1	Zijn de bedrijfscontinuïteitscapaciteiten van de leveranciers en partners onderzocht		
8.3.2	Zijn de middelen voor het herstel geïdentificeerd: mensen, informatie, gebouwen en voorzieningen, uitrusting, IT en communicatiesystemen, transport, financiën, partners en leveranciers.		
8.3.3	Wordt het mitigeren van de onderkende risico's gedefinieerd en worden ze actief geïmplementeerd		
8.4.1	Hebben de bedrijfscontinuïteitsprocedures of plannen deze elementen: communicatieprotocollen, hebben specifieke stappen, flexibel voor iedere mogelijke bedreiging, gericht op het minimaliseren van de gevolgen.		
8.4.2	Bestaan er incidentopvangprocedures met startdrempels en procedures van response		

8.4.3	Bestaat er een procedure voor het signaleren en [blurred] de communicatiemiddelen beschikbaar zullen zijn		
8.4.4	Bestaan bedrijfscontinuïteitsplannen die rollen en [blurred] activiteiten		
8.4.5	Worden de procedures die het herstel aangeven van de activiteiten vastgelegd		
8.5	Wordt regelmatig geoefend en getest, zijn ze [blurred] de oefening opgesteld		
9.1.1	Staat gedefinieerd wat er gemeten dient te [blurred] evalueren		
9.1.1	Zijn de meetresultaten vastgelegd en gerapporteerd aan de verantwoordelijken		
9.1.2	Worden periodieke herbeoordelingen gedaan of [blurred] vereisten geëvalueerd		
9.1.2	Worden post-incidentbeoordelingen uitgevoerd nadat de bedrijfscontinuïteitsprocedures worden geactiveerd		
9.2	Bestaat een auditprogramma, wie bepaalt de timing, verantwoordelijkheden, rapportage, auditcriteria en toepassingsgebied		
9.2	Worden er interne audits uitgevoerd volgens het [blurred] ontstane corrigerende maatregelen		
9.3	Wordt de directiebeoordeling regelmatig uitgevoerd, en worden resultaten vastgelegd in notulen van de vergadering		
9.3	Besloot de directie op alle kritische zaken [blurred]		
10.1	Overweegt de organisatie de gevolgen van [blurred] corrigerende maatregelen te nemen		
10.1	Reageerde de organisatie op elke afwijking		
10.1	Zijn alle afwijkingen vastgelegd, tezamen met de corrigerende maatregelen		