IT Audit Essentials

Rapportage Self Assessment

Uitgevoerd door: Test Bedrijf

Inhoudsopgave

Klantgegevens	
Bedrijfsnaam	Test Bedrijf
Naam invuller	Jan Janssen
Functie	Controller
Telefoon nummer	0123456789
E-mail	joost@itriskcontrol.nl
Naam accountantskantoor	De Accountant
Invul datum	1/10/2018

Algemeen

Het ontwerp, inrichting en werking van de IT-systemen hebben invloeden op de controle. Bijvoorbeeld voor het bepalen van het (pre)auditrisk, de aanpak en uitvoering van de controle, het beoordelen van de processen en de transactiestromen. De inzet van IT gaat veelal gepaard met andere risico's en beheersmaatregelen die nodig zijn om de risico's binnen aanvaardbare grenzen te houden.

Om voldoende zekerheid te krijgen dat de jaarrekening geen afwijkingen van materieel belang bevat en omdat een groot deel van de Administratieve Organisatie en Interne Beheersmaatregelen (AOIB) veelal is ingebed in de opzet en inrichting van de geautomatiseerde systemen, dient ook 'het informatiesysteem', voor zover van belang voor de financiële verslaglegging, in ogenschouw te worden genomen (zie NVCOS 315).

Om de accountant hierin te ondersteunen is een assessment uitgevoerd naar de IT-omgeving en IT beheersmaatregelen. De uitkomsten geven inzicht in de IT-omgeving en de beheersmaatregelen die zijn getroffen. Met deze inzichten beschikt de accountant over een gestructureerde basis om mogelijke risicio's te kunnen bepalen en de aanpak en uitvoering van de controle hierop af te stemmen.

Objecten

Het assessment is gericht op het geven van inzicht in:
- De typering van de automatiseringsomgeving;
- De functiegebieden waarin automatisering wordt toegepast;
- De aanwezige IT-systemen;
- De getroffen beheersmaatregelen.

Doel

Het doel van het assessment is:
- Voorzien in een gestructureerde verzameling en vastlegging van essentiële informatie rondom de IT ten behoeve van en vastlegging in het controledossier;
- Het identificeren van mogelijke aandachtspunten voor de managementletter;
- Het identificeren van mogelijke risico's om de accountant in staat te stellen de aanpak en uitvoering van de controle hierop af te stemmen;
- Het verhogen van de doelmatigheid en doeltreffendheid van de controle.

Daarnaast zijn vragen opgenomen over de Algemene verordening gegevensbescherming (AVG). Het doel hiervan is om op hoofdlijn inzicht te krijgen of de regelgeving bekend is en wordt toegepast, voor zover relevant.

In verband met de toenemende dreigingen van Cybercriminaliteit is een check opgenomen. De check is een hulpmiddel dat om inzicht te krijgen in de staat van cyberbeveiliging in een organisatie. Deze Health Check is vooral gericht op middelgrote bedrijven. Ook is het een leidraad voor controlerend accountants om met hun opdrachtgevers het gesprek over cybersecurity aan te gaan.

Uitvoering

Het assessment is in de vorm van een digitaal self-assessment uitgevoerd. Het assessment is ingevuld door de functionaris,

Controller

waarna de uitkomsten zijn verwerkt en omgezet in deze rapportage. Dit betreft zowel kwalitatieve als kwantitatieve aspecten.

Beperkingen

De mate waarin en de wijze waarop organisaties zijn geautomatiseerd varieert. Situaties zijn zelden gelijk. Aan de kwaliteit van de IT-processen kan en hoeft ook niet in elke organisatie hetzelfde belang te worden toegekend. Om deze redenen kan niet worden uitgegaan van een standaard automatiseringsomgeving en kunnen geen eenduidige en absolute normeringen worden gehanteerd waaraan de kwaliteit van de ITbeheersmaatregelen kan worden getoetst.

Mede hierdoor is het niet mogelijk om aan de uitkomsten een eenduidige en absolute conclusie te geven.

Op basis van in de praktijk toegepaste, gangbare normen en onze ervaringen geven de uitkomsten naar onze mening wel een goed bruikbare indicatie over de aard en omvang van de IT-omgeving en de daarbij getroffen beheersmaatregelen.

Op basis hiervan kan de accountant een overwogen beslissing nemen ten aanzien van mogelijke risico’s, de aanpak en de uitvoering van de controle en het al dan niet instellen van nader (professioneel) onderzoek, indien de uitkomsten van het assessment daartoe aanleiding geven.

Inzake de uitkomsten van de AVG en de Cybersecurity kan met de opdrachtgever worden besproken of en in hoeverre nadere acties noodzakelijk zijn.

De rol van het assessment en deze rapportage is gericht en beperkt tot het systematisch verzamelen en structureren van informatie en het inzichtelijk maken van een aantal mogelijke relevante aandachtspunten.

Een validatie van de antwoorden maakt geen onderdeel uit van het self-assessment.

Uikomsten assessment

In het navolgende zijn de uitkomsten van het assessment opgenomen. Dit betreft:
- Managementsamenvatting;
- Detailbevindingen;
- Bijlage(n).

Managementsamenvatting

Inleiding

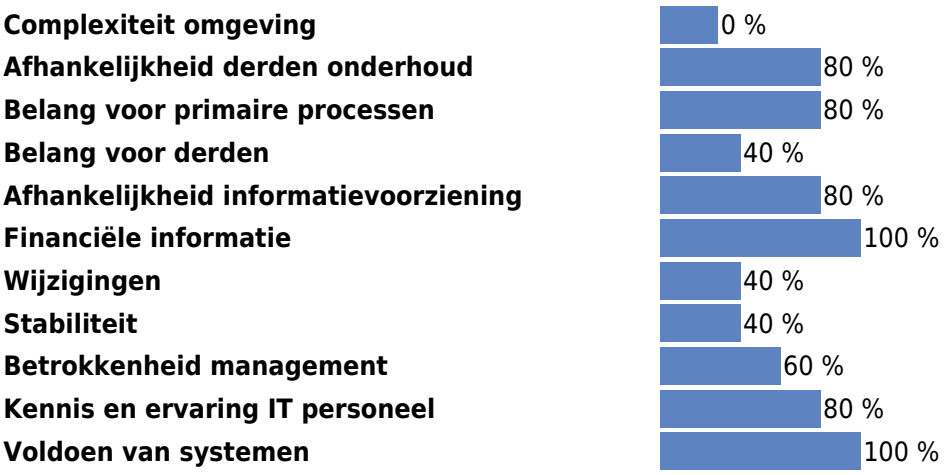
Om de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking te kunnen waarborgen zijn beheersmaatregelen noodzakelijk. De aard en inhoud van de beheersmaatregelen dienen te zijn afgestemd op het belang van de automatisering voor de organisatie. Achtereenvolgens wordt ingegaan op functiegebieden waarin automatisering wordt toegepast, de typering van de automatiseringsomgeving, de gehanteerde werkwijzen en de beheersmaatregelen.

Typering IT omgeving

Op basis van een aantal gesloten vragen is gevraagd de IT-omgeving te typeren. Onderstaande tabel toont de verkregen antwoorden.

Vraag	Antwoord
Hoe beoordeelt u de complexiteit van uw computeromgeving?	Redelijk complex
Hoe afhankelijk bent u van derden voor het onderhoud van systemen en het waarborgen van de beschikbaarheid?	Sterk afhankelijk
Hoe afhankelijk zijn de primaire bedrijfsprocessen van automatisering?	Sterk afhankelijk
Hoe belangrijk is uw automatisering voor derden (klanten, samenwerkingspartners en/of leveranciers)?	Enigzins afhankelijk
Hoe afhankelijk is de financiële informatievoorziening van de betrouwbare werking van uw automatiseringsomgeving?	Sterk afhankelijk
Op welke wijze komt de periodieke financiële informatievoorziening tot stand?	Via overname en bewerkingen van gegevens (bijvoorbeeld in MS Excel)
Hoe vaak worden wijzigingen doorgevoerd in de automatiseringsomgeving?	Weinig wijzigingen
Hoe stabiel zijn uw huidige systemen?	Stabiel, weinig tot geen storingen
In welke mate is het management bewust van het strategisch belang van IT en de bijbehorende risico's?	Management is zich bewust van belang en risicos
Hoe adequaat is de kennis en ervaring van IT-personeel?	Ruim voldoende
In welke mate voldoen de huidige systemen aan de wensen van de organisatie?	Huidige systemen zijn volledig aangesloten en geselecteerd op basis van de wensen uit de organisatie

Om de IT-omgeving te kunnen kwantificeren is op deze antwoorden een berekening uitgevoerd. Onderstaande grafiek toont de uitkomsten van deze berekening, waarbij een schaal van 1 tot 100 is gehanteerd.



De score per onderdeel is een indicatie over het belang van het onderdeel voor de controle. Hoe hoger de score hoe hoger het belang en de mogelijke invloed op de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Bij een hoge score op een onderdeel zullen zwaardere eisen moeten worden gesteld aan de kwaliteit van de beheersmaatregelen op dat onderdeel.

Als op meerdere onderdelen een hoge score wordt gehaald, is dit een indicatie dat er sprake is van een relatieve ‘zware’ IT-omgeving. Bijvoorbeeld in termen van complexiteit, belang voor de organisatie, afhankelijkheid en de mogelijke invloed daarvan op betrouwbaarheid van de geautomatiseerde gegevensverwerking en informatievoorziening.

Op basis van het voorgaande is de relatieve zwaarte van de IT omgeving op een schaal van 1-100 in dit assesment berekend op: **64**. De waarde is gebaseerd op de berekening van het ongewogen gemiddelde van alle onderdelen samen. Naar mate de totaal score hoger is, is er sprake van een ‘zwaardere’ IT-omgeving. Alhoewel geen absolute normen kunnen worden gesteld is het, naar mate de score hoger is, van toenemend belang om aandacht te besteden aan de IT-omgeving.

Algemene beheersmaatregelen

De algemene beheersmaatregelen betreffen maatregelen die van essentieel belang zijn om de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking in de basis te kunnen waarborgen. Dit betreft onder andere functiescheiding, het beheer van wijzigingen, logische en fysieke toegangsbeveiliging en maatregelen inzake continuïteit, backup en recovery.

Aan de hand van een aantal stellingen is in het assessment nagegaan in welke mate is voorzien in essentiële maatregelen. Onderstaande tabel toont de resultaten:

Onderwerp	Ja	Nee	Niet ingevuld
Functiescheidingen	78%	22%	0%
Wijzigingenbeheer	67%	33%	0%
Continuiteit	50%	50%	0%
Beveiliging	75%	25%	0%
Autorisaties	50%	50%	0%

Handreiking controle aanpak

Om toch enigszins te ondersteunen in het kiezen van een controle bieden wij onderstaand een handreiking. Deze handreiking is uitsluitend bedoeld als een grove indicatie. De uiteindelijke keuze van de controle aanpak en de motieven waarop de keuze is gebaseerd is alleen en uitsluitend de verantwoordelijkheid van de externe accountant.
Op basis van een relatie tussen de zwaarte van de IT omgeving en het niveau van de beheersmaatregelen hebben wij onderstaande classificatietabel samengesteld:

	Typering zwaarte IT omgeving		
Kwaliteit beheersmaatregelen	**Laag** (<30)	**Middel** (30<70)	**Hoog** (=>70)
Hoog (=>70 waarbij geen onderdeel <60%)	HL	HM	HH
Middel (=>50 waarbij geen onderdeel <40%)	ML	MM	MH
Laag (Als niet is voldaan aan de criteria voor Hoog en Middel)	LL	LM	LH

Op basis van deze classificatietabel worden de uitkomsten van het assessment als volgt geclassificeerd.

- **Typering zwaarte IT omgeving**: L
- **Niveau van de beheersmaatregelen**: M

Classificatie	ML
Aanbevelingen in Management Letter m.b.t. beheersing:	Neem in de ML aanbevelingen op over relevante tekortkomingen in de Algemene Beheersmaatregelen.
Testen manual controls:	Maatregelen in de IT (beheersmaatregelen en/of application controls) zijn onvoldoende. De aandacht in de controle zal daarom vooral uit moeten gaan naar de door de gebruikers zelf uitgevoerde procedurele - en controlemaatregelen.
Inzet data analyse software:	Bij omvangrijke transactie- en datastromen is de inzet van data analyse software te overwegen.
Testen IT beheersmaatregelen:	
Testen application controls:	

AVG

De vragen met betrekking tot de AVG hebben uitsluitend een inventariserende functie.
Ten aanzien van de AVG zijn de volgende scores verkregen:
Het percentage met ja beantwoorde vragen is 100%, het aantal met nee beantwoorde vragen is 0%, en 0% van de AVG gerelateerde vragen is niet ingevuld.

Een verdere analyse van de antwoorden is binnen deze rapportage niet mogelijk. Wij adviseren u na te gaan of de uitkomsten in lijn zijn met de voor uw organisatie relevante wet- en regelgeving. Indien u niet voldoet is het raadzaam nader onderzoek uit te voeren en waar nodig aanvullende maatregelen te treffen.

Cybersecurity Check

In de check is op een aantal onderwerpen gevraagd aan te geven of een aantal met name genoemde beheersmaatregelen voldoende zijn geïmplementeerd binnen uw organisatie. Dit op basis van stand van zaken op het moment van invullen. Op basis van de verkregen antwoorden worden de volgende risico's onderkend:

Identificatie
U hebt een of meerdere antwoorden met nee of niet beantwoord.
De relevante dreigingen worden niet onderkend. Daardoor is onduidelijk aan welke risico's het bedrijf wordt blootgesteld en welke maatregelen moeten worden genomen.

Bescherming
U hebt een of meerdere antwoorden met nee of niet beantwoord.
Een aanvaller krijgt voet aan de grond in uw organisatie. Bijvoorbeeld doordat medewerkers op links in phishingmails klikken, malware hun (onvoldoende gepatchte) endpoint infecteert en zich vervolgens ongebreideld door het (onvoldoende gesegmenteerde) netwerk kan verspreiden naar andere werkstations en servers.

Detectie
U hebt een of meerdere antwoorden met nee of niet beantwoord.
Incidenten worden niet tijdig opgemerkt, waardoor niet adequaat kan worden opgetreden en de incidenten (en impact daarvan) voortduren.

Reactie
U hebt een of meerdere antwoorden met nee of niet beantwoord.
Inadequate reactie heeft tot gevolg dat de impact van cyberincidenten groter is dan noodzakelijk.

Herstel
U hebt een of meerdere antwoorden met nee of niet beantwoord.
Inadequate reactie heeft tot gevolg dat de impact van cyberincidenten groter is dan noodzakelijk.

Een verdere analyse/advisering is binnen deze rapportage niet mogelijk. Wij adviseren u na te gaan of de uitkomsten in lijn zijn met de voor uw organisatie relevante belangen en waar nodig aanvullende maatregelen te treffen.

Detailbevindingen

Dit hoofdstuk geeft een overzicht van de detailbevindingen. Het betreft de volgende onderdelen:

- Functiescheiding;
- Beheer van wijzigingen;
- Continuïteit, backup en recovery;
- Beveiliging en Autorisaties;
- Cloudcomputing en ASP;
- Webshops/Webportals;
- Thuis - en mobiel werken.
- AVG

Per onderdeel zijn stellingen over de aanwezigheid van beheersmaatregelen voorgelegd, waarop met ‘Ja’ of ‘Nee’ kon worden geantwoord. Daarbij is ook de mogelijkheid geboden om geen antwoord te geven.

Bij elke stelling is tevens de mogelijkheid geboden een toelichting te geven op het antwoord, bijvoorbeeld ter verduidelijking. Voor een zo goed mogelijke interpretatie van het antwoord op een stelling, is het van belang om deze toelichting te lezen.

Verder is aan het eind van elk onderdeel de gelegenheid gegeven om desgewenst nog een nadere toelichting en/of aanvullende opmerkingen over het onderwerp te geven. Als daarvan gebruik is gemaakt is dit in een tekstvak schuingedrukt weergegeven. Als geen gebruik is gemaakt van deze mogelijkheid is het tekstvak voorzien van de tekst '*Geen aanvullende opmerkingen*'.

Functiescheiding

Belang

Functiescheiding is noodzakelijk om mogelijke belangenverstrengeling te helpen voorkomen. Dit betreft onder andere de scheiding van taken en verantwoordelijkheden binnen de automatiseringsafdeling zelf en de scheiding van taken en verantwoordelijkheden tussen medewerkers van de automatiseringsafdeling en functionele gebruikers in het financiële domein. In kleinere omgeving is een vermenging niet altijd te voorkomen. Een adequate monitoring en controle op de activiteiten is dan nodig.

Maatregelen

In het assessment zijn de volgende antwoorden verkregen:

Maatregel	Antwoord	Toelichting
De automatiseringsafdeling functioneert onafhankelijk van de andere bedrijfsfuncties	Ja	
Het technisch beheer van systemen en applicaties is gescheiden van het functioneel beheer	Ja	
Er is een helpdesk voor het registreren en oplossen van incidenten	Ja	
Er zijn processen ingericht voor configuratiemanagement	Nee	
Goedkeuren van wijzigingen in systemen/applicaties is gescheiden van technisch en functioneel beheer	Ja	
Beheer van applicaties en systemen is gescheiden van de ontwikkeling van software	Ja	
De automatiseringsafdeling en gebruikers zijn functioneel gescheiden	Nee	
Financiële gegevensbestanden zijn voor automatiseringspersoneel beveiligd tegen toegang	Ja	
De integriteit van data wordt regelmatig gecontroleerd, bijvoorbeeld door verbandscontroles	Ja	Via allerlei excelsheets worden verbanden gelegd

Functies en taken	Naam / Functie	Toelichting
Technisch systeembeheer	Jan Janssen	
Technisch applicatiebeheer	Piet Pietersen	
Netwerkbeheer	Externe ICT Partij	
Functioneel applicatiebeheer	Wim De Vries	
Databasemanagementbeheer	Wim de Vries	

Beheer van wijzigingen

Belang

Alle wijzigingen, inclusief noodmaatregelen en -patches, op de operationele infrastructuur en applicaties dienen beheerst te worden doorgevoerd. Beheerst doorvoeren van wijzigingen houdt in dat wijzigingen worden geregistreerd, beoordeeld en goedgekeurd voordat de wijzigingen worden doorgevoerd. Na afloop worden de doorgevoerde wijzigingen gecontroleerd. Dit minimaliseert het risico van een verstoring op de stabiliteit en integriteit van de operationele omgeving. Het is daarom van belang te beschikken over een gestructureerd wijzigingenbeheer waarbij wijzigingen op een geplande en beheerste wijze worden doorgevoerd om mogelijke verstoringen te beperken cq. te voorkomen.

Maatregelen

In het assessment zijn de volgende antwoorden verkregen:

Maatregel	Antwoord	Toelichting
Wijzigingen in programmatuur worden uitgevoerd op basis van geautoriseerde procedures	Nee	
Het ontwerpen, testen en goedkeuren van systemen verloopt via geautoriseerde procedures	Ja	
De procedures voor het ontwikkelen,testen, accepteren en overdragen van software zijn gedocumenteerd	Nee	
Testprocedures worden buiten de operationele omgeving uitgevoerd	Ja	
De programmatuur (inclusief parameters) is beveiligd tegen aanpassingen door gebruikers	Ja	
Wijzigingen in systeeminrichting, parameters, stamtabellen e.d., zijn inzichtelijk via een 'audit trail'	Ja	

Activiteit	Naam / Functie	Toelichting
Opstellen wijzigingsverzoeken	Jan Janssen	
Goedkeuren wijzigingsverzoeken	Directeur	
Ontwikken/aanpassen applicaties	Externe ICT Partij	
Testen wijzigingen	Jan Janssen	
Goedkeuren wijzigingen	Jan Janssen	
Implementatie wijzigingen	Jan Janssen	

Continuïteit, backup en recovery

Belang

Het waarborgen van de continue beschikbaarheid van de IT-voorzieningen vereist het ontwikkelen, onderhouden en testen van continuiteitsplannen, het opslaan van backup op een externe lokatie en het periodiek trainen op de werking van de plannen. Als sprake is van een grote afhankelijkheid zal een verstoring in de IT-voorzieningen direct leiden tot stagnatie van een of meerdere primaire bedrijfsprocessen. Bij een dergelijke afhankelijkheid is het noodzakelijk te beschikken over hierop afgestemde ITcontinuïteitsvoorzieningen.

Maatregelen

In het assessment zijn de volgende antwoorden verkregen:

Continuïteitsplan	Antwoord	Toelichting
Door het management zijn de eisen van beschikbaarheid vastgesteld	Ja	
Een continuïteitsplan is beschikbaar	Nee	
Het continuïteitsplan voldoet aan de eisen van het management	Nee	
Het continuïteitsplan wordt periodiek getest	Nee	

Backup	Antwoord	Toelichting
Periodiek worden backups gemaakt	Ja	
De backup cyclus is afgestemd op de eisen van het management	Ja	
In de backup cyclus is voorzien in de backup van OS, applicaties en data	Ja	
Backups worden op een externe locatie opgeslagen	Ja	
De geschiktheid van datadragers wordt periodiek gecontroleerd	Ja	

Recovery	Antwoord	Toelichting
Kritische IT-middelen en personen zijn vastgesteld	Ja	
De volgorde waarin systemen moeten worden hersteld, staat vast	Nee	
Herstelprocedures zijn formeel vastgesteld	Nee	
Herstelprocedures worden regelmatig getest en geëvalueerd	Nee	
Alle betrokken personen zijn geïnformeerd en getraind	Nee	

Beveiliging en Authorisaties

Belang

De noodzaak om de integriteit van informatie te waarborgen en de IT-middelen te beschermen maakt systeembeveiliging noodzakelijk. Dit betreft zowel de fysieke beveiliging als de logische toegang(beveiliging). Bijvoorbeeld de beveiliging van de IT-omgeving tegen onbevoegde toegang en het hanteren van beveiligingsbeleid, standaarden en procedures. Het betreft ook het monitoren en de periodieke toetsing en implementatie van correctieve maatregelen als zwakheden worden aangetroffen of beveiligingsincidenten zich hebben voorgedaan. Effectieve systeembeveiliging beschermt de IT-middelen zodat het risico van impact op de bedrijfsprocessen wordt geminimaliseerd.

Maatregelen

In het assessment zijn de volgende antwoorden verkregen:

Beveiligingsbeleid en −richtlijnen	Antwoord	Toelichting
De directie heeft formele richtlijnen vastgesteld	Ja	
De naleving van de richtlijnen wordt periodiek getoetst	Nee	
Overtredingen worden gerapporteerd aan de directie	Ja	

Systeem beveiliging	Antwoord	Toelichting
Systemen zijn beveiligd tegen onbevoegde toegang van buitenaf	Ja	
De netwerken en systemen zijn beveiligd tegen virussen, malware, spyware, trojan horses, DOS−aanvallen, etc	Ja	AVG
Voor de beveiliging van hulpmiddelen, die worden gebruikt voor de beveiliging, zijn procedures opgesteld	Nee	
Op de uitwisseling van gevoelige informatie zijn procedures van toepassing	Ja	
Voor de controle op systeemlogs zijn procedures aanwezig	Nee	

Fysieke beveiliging	Antwoord	Toelichting
Bij de locatie van de serverruimte is rekening gehouden met het belang van de ruimte	Ja	Extern
De fysieke toegang tot de serverruimte wordt beheerst	Ja	Extern
De serverruimte is afdoende beschermd tegen fysieke dreigingen, waaronder brand en wateroverlast	Ja	Extern
De serverruimte is voorzien van noodstroomvoorzieningen	Ja	Extern

Autorisaties	Antwoord	Toelichting
Gebruikers krijgen uitsluitend de bevoegdheden die voor de functie noodzakelijk zijn	Ja	
Voor het aanvragen en wijzigen van autorisaties zijn formele procedures aanwezig	Ja	
De toegang tot bestanden, programma's e.d. is beveiligd, bijvoorbeeld door passwords en/of toegangsmiddelen	Ja	
De systemen dwingen af dat passwords periodiek moeten worden gewijzigd	Nee	
Periodiek worden autorisatie instellingen getoetst	Nee	
Periodiek wordt een controle uitgevoerd op de toegangslogs	Nee	

Welke functionarissen hebben 'super-user' rechten en voor welk systeem gelden deze?

Systeem/Applicatie	Naam/Functie Super user (Admin)	Toelichting
Exact Globe	Jan Janssen, Controller	

Automatisering extern

Belang

Automatiseringsvoorzieningen zijn tegenwoordig niet alleen ondergebracht binnen de muren van een organisatie. Meer en meer wordt ook gebruik gemaakt van IT-voorzieningen die bij externe partijen zijn ondergebracht. Als met automatisering 'buiten de muren' wordt getreden is het van belang om aandacht te schenken aan een aantal specifieke beheersmaatregelen. Om deze reden zijn een aantal stellingen over essentiële beheersmaatregelen voorgelegd.

Maatregelen

In het assessment zijn de volgende antwoorden verkregen:

Cloud/ASP

Maatregel	Antwoord	Toelichting
De afspraken met de provider(s) zijn schriftelijk vastgelegd, bijvoorbeeld in een SLA	Ja	
Voor deze systemen zijn waarborgen getroffen om de continue beschikbaarheid te kunnen waarborgen	Ja	
Bij de de keuze van de provider is rekening gehouden met de geografische locatie van de dataopslag ivm privacywetgeving	Ja	
Voor het datacenter, waar de systemen/applicaties zijn ondergebracht, is een SAS70/ISAE 3402 verklaring afgegeven	Ja	
Met de provider zijn afspraken gemaakt over het overdragen van de data als de overeenkomst wordt beëindigd	Ja	

Webshop/Webportal

Maatregel	Antwoord	Toelichting
Biedt u derden, bijvoorbeeld (klanten en/of leveranciers) toegang tot (delen van) uw systemen, bijvoorbeeld via een Webshop/Webportal?	Nee	

Mobiel en thuiswerken

Maatregel	Antwoord	Toelichting
Voor thuis- en mobiel werken zijn beleid, richtlijnen en procedures opgesteld	Nee	
Er zijn voldoende maatregelen getroffen zodat thuiswerken op een veilige manier kan plaatsvinden	Nee	
Mobiele apparaten zijn voorzien van mechanismen om ongeautoriseerde toegang te voorkomen	Ja	

Data op mobiele devices worden versleuteld opgeslagen	Nee	
In geval van verlies of diefstal zijn maatregelen getroffen om de schade en gevolgen (bijv. dataverlies) te beperken	Nee	

AVG

Belang

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt –meer dan nu –op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden. Als organisatie moet u voldoen aan een aantal voorwaarden. Als u niet voldoet loopt u de kans op hoge boetes, kunt u aansprakelijk worden gesteld en/of loopt u de kans op imagoschade. Dit kan van invloed zijn op de financiële verantwoording. Om inzicht te krijgen of de AVG voor uw organisatie van belang is onderstaand een selectie van een aantal vragen. Meer informatie over de AVG vindt u bij de Autoriteit Persoonsgegevens (AP).

Maatregelen

In het assessment zijn de volgende antwoorden verkregen:

Maatregel	Antwoord	Toelichting
Verwerkt u persoonsgegevens?	Ja	
Kent u de rechten van betrokkenen?	Ja	
Heeft u de gegevensverwerking in kaart?	Ja	
Heeft u een procedure voor het registreren en melden van datalekken?	Ja	
Heeft u uw gegevensverwerking uitbesteed aan een verwerker?	Ja	
Heeft u toestemming van betrokkenen?	Ja	

Cybersecurity

Cybercrime is big business. Malafide organisaties verdienen veel geld door organisaties te hacken. Vaak is het een kwestie van tijd voordat een organisatie te maken krijgt met cybercrime. En niet zelden ligt daar menselijk handelen aan ten grondslag. De vraag hoe organisaties zich tegen cybercrime kunnen wapenen is dan ook een terechte. Absolute veiligheid bestaat echter niet, maar bewustwording bij bestuurders en werknemers is nog steeds een belangrijk wapen in de strijd.

Cybersecurity Health Check

De check is een hulpmiddel dat u in staat stelt inzicht te krijgen in de staat van cyberbeveiliging van uw organisatie. Deze Health Check is vooral gericht op middelgrote bedrijven. Ook is het een leidraad voor controlerend accountants om met hun opdrachtgevers het gesprek over cybersecurity aan te gaan.

De Health Check is op verzoek van de Cyber Security Raad ontwikkeld door specialisten van vier grote accountantsorganisaties. De Cybersecurity Health Check, is op initiatief van de Cyber Security Raad door specialisten van een aantal accountantskantoren opgesteld. Voor meer informatie kunt u terecht op de website https://www.cybersecurityraad.nl . De check is geen uitputtende lijst, maar bedoeld als een goede start om de belangrijkste cyberrisco's in beeld te brengen en te mitigeren.

In de check is gevraagd aan te geven of een aantal met name genoemde beheersmaatregelen voldoende zijn geïmplementeerd binnen uw organisatie. Dit op basis van stand van zaken op het moment van invullen. Hierbij zijn de volgende antwoorden verkregen:

Identificatie

Maatregel	Antwoord	Toelichting
Is de verantwoordelijkheid voor cybersecurity binnen de directie belegd en wordt cybersecurity periodiek binnen de directie besproken?	Nee	
Is binnen uw organisatie inzichtelijk wat uw belangrijkste kroonjuwelen zijn (webshop, operationele en financiële data, persoonsgegevens klanten) en wat het effect van een cyberaanval op deze kroonjuwelen kan zijn?	Nee	
Zijn de belangrijkste cyberrisico’s en -dreigingen in kaart gebracht en worden deze periodiek geëvalueerd vanuit een strategisch, financieel, operationeel, reputatie en compliance (bv. AVG) perspectief inclusief derde partijen?	Nee	

U hebt een of meerdere antwoorden met nee of niet beantwoord.
De relevante dreigingen worden niet onderkend. Daardoor is onduidelijk aan welke risico's het bedrijf wordt blootgesteld en welke maatregelen moeten worden genomen.

Bescherming

Maatregel	Antwoord	Toelichting
Scholen uw medewerkers zich tenminste jaarlijks bij, om op de hoogte te blijven van recente ontwikkelingen en 'do's & don'ts' op securitygebied voor hun functie (zowel IT als non-IT)?	Nee	
Is bij zowel u als een eventuele derde partij het patch management (bijwerken, testen en installeren van software) op orde?	Ja	
Is bij zowel u als een eventuele derde partij het toegangsbeheer (incl. intrekken toegang van gebruikers na functiewisseling of - beëindiging) op orde?	Nee	
Is bij zowel u als een eventuele derde partij het maken van back-ups op orde?	Ja	
Worden deze periodiek uitgevoerd en wordt de effectiviteit ervan regelmatig getest? Zo nee, wat doet u wel aan eventuele periodieke controles?	Nee	
Heeft uw organisatie effectieve maatregelen in gebruik voor netwerksegmentatie, endpoint security, en (D)DoS-mitigatie. Zijn systemen voldoende robuust en wordt gebruik gemaakt van 2FA (bv: wachtwoord en code via SMS) voor authenticatie op gevoelige systemen?	Nee	

U hebt een of meerdere antwoorden met nee of niet beantwoord.
Een aanvaller krijgt voet aan de grond in uw organisatie. Bijvoorbeeld doordat medewerkers op links in phishingmails klikken, malware hun (onvoldoende gepatchte) endpoint infecteert en zich vervolgens ongebreideld door het (onvoldoende gesegmenteerde) netwerk kan verspreiden naar andere werkstations en servers.

Detectie

Maatregel	Antwoord	Toelichting
Maakt uw organisatie gebruik van logging (log files), al dan niet centraal geaggregeerd? Wordt deze ook actief geanalyseerd, zodat monitoring van incidenten plaatsvindt?	Nee	
Is uw organisatie in staat om de dreiging van ransomware (WannaCry, Petya) te detecteren, bijvoorbeeld door het inzetten van monitoring software op computer-, server- en/of netwerkniveau?	Ja	

Is uw organisatie in staat om de dreiging van virussen en trojans (Remote Access Tools) te detecteren, bijvoorbeeld door het inzetten van monitoring software op computer-, server- en/of netwerkniveau?	Ja	
Is uw organisatie in staat om de dreiging van diefstal van informatie (bedrijfsgeheimen) te detecteren, bijvoorbeeld door het inzetten van monitoring software op computer-, server- en/of netwerkniveau?	Nee	
Is uw organisatie in staat om de dreiging van ongeautoriseerde toegang tot servers en/of informatie te detecteren, bijvoorbeeld door het inzetten van monitoring software op computer-, server- en/of netwerkniveau?	Ja	
Toetst uw organisatie de effectiviteit van de getroffen beveiligingsmaatregelen door het uitvoeren van een kwetsbaarhedenscan?	Nee	
Toetst uw organisatie de effectiviteit van de getroffen beveiligingsmaatregelen door het uitvoeren van penetratietesten?	Nee	
Toetst uw organisatie de effectiviteit van de getroffen beveiligingsmaatregelen door het uitvoeren van red-teaming?	Nee	

U hebt een of meerdere antwoorden met nee of niet beantwoord.
Incidenten worden niet tijdig opgemerkt, waardoor niet adequaat kan worden opgetreden en de incidenten (en impact daarvan) voortduren.

Reactie

Maatregel	Antwoord	Toelichting
Heeft uw organisatie een communicatieplan opgesteld om belanghebbenden (zoals de juridische afdeling, de pers, leveranciers, afnemers, personeel, overheid, Autoriteit Persoonsgegevens, etc.) tijdig en adequaat te informeren over een cyberincident?	Nee	
Heeft uw organisatie een crisisplan opgesteld om de impact van cyberincidenten te beperken en het incident zelf uiteindelijk te verhelpen en is helder wie welke rol daarin heeft?	Nee	

Oefent uw organisatie periodiek (bijvoorbeeld een keer per jaar) het reageren op een gesimuleerd cyberincident en bespreekt u de uitkomsten daarvan in het bestuur voor het verbeteren van het communicatie- en crisisplan?	Nee	

U hebt een of meerdere antwoorden met nee of niet beantwoord.
Inadequate reactie heeft tot gevolg dat de impact van cyberincidenten groter is dan noodzakelijk.

Herstel

Maatregel	Antwoord	Toelichting
Heeft uw organisatie een herstelplan opgesteld, dat u in staat stelt op tijd de bedrijfsvoering te hervatten (voordat de schade te groot is)?	Nee	
Zijn uw back-upvoorzieningen zodanig ingericht dat u snel en efficiënt getroffen systemen kunt herstellen naar normale operatie en test u dit regelmatig?	Ja	
Heeft uw organisatie processen en middelen om te leren van opgetreden cyberincidenten om deze in de toekomst te voorkomen, sneller te detecteren of beter op te reageren?	Ja	

U hebt een of meerdere antwoorden met nee of niet beantwoord.
Inadequate reactie heeft tot gevolg dat de impact van cyberincidenten groter is dan noodzakelijk.

Een verdere analyse/advisering is binnen deze rapportage niet mogelijk. Wij adviseren u na te gaan of de uitkomsten in lijn zijn met de voor uw organisatie relevante belangen en waar nodig aanvullende maatregelen te treffen.

Afsluitende opmerkingen assessment

Aan het eind van het assesment is de gelegenheid gegeven om desgewenst nog een nadere toelichting en/of aanvullende opmerkingen te geven.

Bijlage: IT Omgeving

Belang
Deze bijlage geeft een overzicht van de IT-omgeving. Dit betreft:

- Servers en Operatingsystemen;
- Databasemanagement systemen;
- Bescherming tegen virussen, inbraken en DDOS e.d.;

Servers en Operatingsystemen
De volgende gegevens zijn opgegeven bij de vraag over welke type servers u gebruikt, en welke Operating Systemen en versies deze servers gebruiken:

Zie bijlage met beschrijving van het serverpark en de operating systemen

Databasemanagement systemen
De volgende gegevens zijn opgegeven bij de vraag over welke Databasemanagement Systemen worden gebruikt en waarvoor deze worden gebruikt:

Zie bijlage

Informatiebeveiliging
De volgende gegevens zijn opgegeven bij de vraag over welke maatregelen zijn getroffen voor het beveiligen van uw informatievoorziening:

AVG hebben wj hiervoor als Tool

Soorten werkplekken

Soort werkplek	Aanwezig	Aantal	Operating systeem	Toelichting
PC Fat client	Ja	16	Microsoft, windows 7	
PC Thin client	Nee			
Laptop	Ja	4	Microsoft, windows 7	
Tablet	Nee			
Smartphone	Ja	2	Apple	
Overige apparatuur	Nee			
Totaal		22		

Bijlage: Functiegebieden

Onderstaande tabel geeft een overzicht van de functiegebieden waarin automatisering wordt ingezet en de pakketten die daarbij worden gebruikt. Volledigheidshalve zijn alle functiegebieden vanuit het assessment opgenomen in de tabel, zodat ook zichtbaar is in welke functiegebieden geen gebruik wordt gemaakt van automatisering.

Functiegebied	Wordt gebruikt	Pakket
Financieel	Ja	Exact Globe
Logistiek	Nee	
Inkoop	Ja	Exact Globe
Verkoop	Ja	Exact Globe
Productie	Nee	
Voorraad	Nee	
Service		
Personeelszaken	Ja	AFAS
Salaris	Ja	ADP
CRM		
CSM	Nee	
Kantoorautomatisering	Ja	Microsoft office 2016
Webverkoop	Nee	
Informatiemanagement/BI	Nee	
Overig	Nee	

Het aantal geautomatiseerde werkplekken bedraagt: 22.

Het aantal functiegebieden in combinatie met het aantal werkplekken geeft een indicatie van de mate waarin automatisering deel uitmaakt van de bedrijfsprocessen. In het algemeen geldt hierbij dat naar mate het aantal gebieden hoger en het aantal werkplekken hoog is, ook het belang en rol van automatisering hoger zal zijn en dus aandacht behoeft.

Als de automatisering in de functiegebieden wordt ingevuld door één en hetzelfde pakket is er sprake van een zogenaamde ERP-pakket. Een dergelijk pakket wordt veelal vanuit een ‘centraal’ punt en een gemeenschappelijke kijk op de bedrijfsprocessen en besturing en beheersing daarvan, ingericht en onderhouden. Vanuit de controle is het in dergelijke omgevingen vooral van belang om aandacht te schenken aan de inrichting van het pakket, waaronder parameters, stamgegevens en de relevante application controls.

Als de automatisering in de functiegebieden wordt ingevuld door meerdere pakketten kan het noodzakelijk zijn de inrichting en relevante application controls afzonderlijk te beoordelen. Verder kan er sprake zijn van geautomatiseerde interfaces. Dergelijke interfaces zijn bedoeld om gegevens tussen de pakketten uit te wisselen. Naast de inrichting van de, voor de controle relevante, pakketten zelf, dient in deze gevallen aandacht te worden besteed aan de opzet van de relevante interfaces en de controles waarin is voorzien om de betrouwbare uitwisseling van gegevens te kunnen waarborgen.

Bijlage: Digitale bestanden Om de uitkomsten van het assessment zo goed mogelijk te kunnen interpreteren is in het assessment gevraagd om, voor zover beschikbaar, aanvullende documenten met het assessment mee te sturen, bijvoorbeeld een schema van het IT landschap en procedure beschrijvingen. Als de klant hiervan gebruik heeft gemaakt, worden de aangeleverde documenten in een afzonderlijk bestand met de rapportage meegeleverd.