IT Audit in de MKB controlepraktijk

Ervaringen en inzichten

Webbased Self Assessments

Juni 2013

Samenvatting

Het belang van IT Audit voor de accountant
De accountant heeft zelf steeds meer behoefte aan inzicht in de kwaliteit van de IT-systemen bij cliënten en de toereikendheid van de beheersmaatregelen. Ook in publicaties van de Autoriteit Financiële Markten (AFM) en de Nederlandse Beroepsorganisatie van Accountants (NBA) wordt het toenemende belang van IT voor de accountant onder de aandacht gebracht.

De praktijk: 'Kloof' tussen belang en mogelijkheden
De accountant beschikt vaak zelf niet over de benodigde kennis, ervaring en hulpmiddelen, om geheel zelfstandig een onderzoek naar de kwaliteit van de IT-systemen en beheersmaatregelen uit te voeren. De inschakeling van een deskundige (IT-auditor) is echter niet vanzelfsprekend. Belemmeringen liggen onder meer in de ruimte in het budget en het bestaan van een kennis- en verwachtingskloof tussen accountant en IT-auditor. Er is al snel sprake van een kloof.

Webbased self assessments
Om 'de kloof' te helpen dichten heeft IT Risk Control onder andere webbased self assessments ontwikkeld. De self assessments maken het mogelijk om snel, doeltreffend en gestructureerd informatie te verzamelen over de IT-omgeving en beheersmaatregelen bij cliënten. Met de inzet van de assessments kan op een kosteneffectieve wijze een eerste stap worden gezet zetten in het vergaren van relevante informatie en op professionele manier gestructureerd inzicht krijgen in mogelijke risico's en de controle aanpak en uitvoering daarop afstemmen en zo een begin te maken met het dichten van de 'kloof'. Een van de assessments die wij hebben ontwikkeld is het General IT Assessment. Dit assessment is gebaseerd op COBIT[1] en vult de volgende behoefte van de accountant in:

- Inzicht in de IT organisatie en de IT systemen van de cliënt;
- Inzicht in de kwaliteit van de beheersmaatregelen;
- Ondersteuning keuze controle aanpak;
- Bieden van een basis voor een nadere gerichte toetsing van de maatregelen;
- Aandachtspunten voor de management letter;
- Bijdrage aan dossiervorming.

Ervaringen en inzichten
Dit rapport gaat over een aantal ervaringen, dat wij hebben opgedaan met de inzet van 190 General IT Assessments, over de periode 2009-2012, in opdracht van accountantskantoren bij hun cliënten.

Enkele inhoudelijke bevindingen/conclusies zijn:
- Veel cliënten overschatten het niveau waarop ze de IT beheersmaatregelen hebben georganiseerd. Bij inschatting van het CobiT-niveau wordt een hoger niveau geschat dan blijkt uit de beantwoording van de toets vragen die ter verificatie zijn gesteld;
- 30 % van de bedrijven beschikt niet over een informatiestrategie;
- 80 % van de bedrijven heeft geen raamwerk voor risico analyse;
- Bij bedrijven die aangeven dat ze sterk afhankelijk zijn van ICT beschikt 75 % niet over een continuïteitsplan;
- In 75 % van de gevallen is er sprake van koppelingen, voor het uitwisselen van gegevens tussen systemen;

[1] Zie www.isaca.org

- Bij 40 % van de applicaties is sprake van maatwerk;
- 35 % beschikt niet over procedures voor het beheer van wijzigingen in IT systemen;
- Ten tijde van de invulling van de assessments was een kleine 60% van de systemen al langer dan 5 jaar in gebruik.

Impact voor de accountant

Uit de assessments blijkt, dat cliënten zich op de meeste hoofdvragen van de COBIT gebieden hoger inschalen, dan door feitelijke maatregelen kan worden aangetoond, dit uitgezonderd de fysieke beveiliging. Vooral op het gebied van beleid, documentatie en methodieken schieten zij tekort. Dit hoeft niet te betekenen, dat de cliënt onvoldoende maatregelen heeft getroffen, maar deze maatregelen zijn dan vaak ad hoc van aard, niet goed gedocumenteerd en daardoor minder (of niet) zichtbaar en aantoonbaar.

Gevolgen voor audit en Management letter

Mits de accountant kan vaststellen, dat daadwerkelijk maatregelen getroffen zijn en gedurende de controleperiode ook hebben gewerkt, dan hoeft het ontbreken van beleid en dergelijke geen onoverkomelijk probleem te zijn voor een systeemgerichte controle aanpak. Het is wel van belang dit te melden in de management letter en bij de Raad van Commissarissen onder de aandacht brengen. Tevens moet de accountant melden als de cliënt risico's loopt op het gebied van continuïteit en betrouwbaarheid, door onvoldoende beheersmaatregelen.

Enkele specifieke consequenties voor de audit aanpak van de bevindingen

Uit de uitkomsten blijkt, dat 75% van de systemen gekoppeld zijn. Voor de audit betekent dit, dat vastgesteld moet worden dat de gegevensuitwisseling[2] tussen de systemen juist, volledig en niet dubbel moet zijn.

Voorts blijkt dat bij 40% van de systemen sprake is van maatwerk. Dit betekent dat de accountant in zijn controle specifiek inzicht moet krijgen in de opzet en werking van de controls in deze aangepaste systemen en dat hij extra kritisch moet zijn als hij op de output wil steunen. Uiteraard moet de accountant vaststellen dat de cliënt wijzigingen in de software goed beheert.

Tot slot

Naast het delen van kennis en inzichten die zijn opgedaan willen wij vooral ook laten zien dat door middel van webbased assessments, met zeer beperkte middelen toch een belangrijke behoefte van de accountant kan worden ingevuld. De assessments maken het mogelijk om doelmatig en doeltreffend het onderwerp IT in relatie tot de controle te adresseren. Voor cliënten biedt het een effectieve manier van zelfreflectie over de rol en het belang van IT in de organisatie.

In combinatie met een proactieve houding van de accountant om de uitkomsten van het assessment in het bredere perspectief van het belang van de cliënt te plaatsen en het initiatief om daarover met de cliënt van gedachten te wisselen biedt de accountant toegevoegde waarde en onderscheidend vermogen. Zaken waar de cliënt vandaag de dag om vraagt.

Wij spreken de verwachting uit met onze assessments aanpak en deze rapportage, vanuit ons vakgebied IT Audit, bij te dragen aan de ontwikkelingen in de accountancymarkt en de uitdagingen die daar liggen.

IT Risk Control BV

[2] Zie http://www.itriskcontrol.nl/qa/interfaces/

Inhoudsopgave

Samenvatting 2
Inleiding 5
I Beheerprocessen en beheersmaatregelen 8
Opzet en structuur General IT Assessment 9
P01 Informatiestrategie 11
P09 Risicomanagement 13
AI6 Wijzigingenbeheer 15
DS4 Continuïteitsbeheer 17
DS5 Systeembeveiliging 21
DS11 Gegevensbeheer 24
DS12 Fysieke beveiliging 26
II Sectoren, branches, typering en software omgeving 28
Branches/sectoren 29
Typering automatiseringsomgeving 30
Koppelingen 34
Maatwerk of standaard 35
Ouderdom van de pakketten 36

Inleiding

Over IT Risk Control BV

IT Risk Control BV is een professionele dienstverlener van IT-auditdiensten, IT-audittools en IT-adviesdiensten. Onze kracht ligt in een innovatieve aanpak, de manier van denken en werken, om een zo hoog mogelijke kwaliteit en toegevoegde waarde aan onze cliënten te leveren.

Een van de segmenten waarin wij actief zijn is de Accountancymarkt. Daarbij ondersteunen wij kantoren[3], die zelf niet over IT audit kennis beschikken, met onze tools en diensten.

Het belang van IT (audit) voor de accountant

De betrouwbaarheid van de financiële verantwoording is in toenemende mate afhankelijk van de kwaliteit van de IT-systemen en de beheersmaatregelen. Bij de interim- en eindejaar controle heeft de accountant daarom behoefte aan inzicht in de kwaliteit van de IT-systemen bij cliënten en de toereikendheid van de beheersmaatregelen. Dat het belang van IT voor de accountant toeneemt, blijkt verder onder meer uit:

1) Themaonderzoek niet-OOB-accountants-kantoren 2013 door de Autoriteit Financiële Markten (AFM)[4]. Met dit onderzoek wil de AFM een duidelijk beeld krijgen van de kwaliteit van de wettelijke controles die worden uitgevoerd door accountantskantoren met een niet-OOB-vergunning. De aandacht van de accountant voor de IT-omgeving van cliënten is daarbij één van de punten waar specifiek naar wordt gekeken.
2) De Nederlandse Beroepsorganisatie van Accountants (NBA) benadrukt in het Visiedocument MKB-accountant 2020[5] het belang van IT. Daarin wordt onder andere gesteld: "Controle kan onmogelijk om de IT heen. Er zijn nieuwe technieken en tools nodig voor data analyse en monitoring. Dit vereist gewijzigde kennis en vaardigheden van de accountant".

Naast deze vakinhoudelijke invalshoeken verwachten cliënten meer en meer een proactieve houding van de accountant bij vraagstukken, ook als het om IT gaat. Bijvoorbeeld bij vragen zoals:
- Is de kwaliteit van de IT-systemen in lijn met het bedrijfsbelang?
- Hoe doeltreffend en doelmatig is de inrichting en het beheer van de IT-systemen?
- Waar liggen mogelijkheden tot verbetering, bijvoorbeeld op basis van 'good Practices'?

Een laatste reden voor de accountant om meer aandacht aan IT te besteden zijn ontwikkelingen met mogelijk ingrijpende gevolgen voor de bestaande bedrijfsmodellen van kantoren. Voorbeelden zijn: Standard Business Reporting, Data-Analyse, Proces Mining, Cloud computing en Continous Auditing.

Kortom redenen genoeg om nader aandacht te schenken aan IT bij de cliënt.

De praktijk: 'Kloof' tussen belang en mogelijkheden

De accountant beschikt veelal zelf niet over de benodigde kennis, ervaring en hulpmiddelen, om geheel zelfstandig een onderzoek naar de kwaliteit van de IT-systemen en beheersmaatregelen uit te voeren. De inschakeling van een deskundige (IT-auditor) is echter niet vanzelfsprekend. Belemmeringen zijn onder meer:
- het controlebudget laat de inzet niet of maar zeer beperkt toe;
- een beperkte inzet geeft weinig mogelijkheden voor het leveren van toegevoegde waarde;
- de cliënt is niet bereid het budget aan te passen voor een uitgebreidere inzet;
- er is een kennis- en verwachtingskloof tussen accountant en IT-auditor.

[3] Voor een overzicht van klanten in de accountancybranche zie http://www.itriskcontrol.nl/klanten/
[4] http://www.afm.nl/nl/nieuws/2013/feb/niet-oob.aspx
[5] MKB-accountant 2020, Visiedocument voor openbaar accountants werkzaam in het MKB, Maart 2013

In meer kleinschalige controleomgevingen ontstaat verder al snel een scheve verhouding tussen de tijd die de IT-auditor beschikbaar heeft voor het daadwerkelijk onderzoek en de tijd die besteed moet worden aan, bijvoorbeeld:
- het verkrijgen van cliëntkennis;
- het verzamelen van gegevens, interviews en het doornemen documentatie;
- het uitwerken en verifiëren van gespreksverslagen;
- het opstellen en bespreken van (concept) rapportages;
- de dossiervorming.

Samenvattend: Het belang is er wel, maar binnen de gegeven omstandigheden zijn de mogelijkheden beperkt ('de kloof').

Deze belemmeringen en praktische bezwaren worden vaak als zo vanzelfsprekend beschouwd, dat de aandacht voor IT en de inzet van een IT-auditor al bij voorbaat uit het aandachtsgebied van de accountant verdwijnt. Vak-gerelateerde risico's en het niet benutten van mogelijkheden kunnen het gevolg zijn. Bijvoorbeeld mogelijkheden voor het verhogen van de doelmatigheid van de controle en/of het verbeteren van de dienstverlening aan de cliënt. Zaken waarnaar cliënten juist in deze tijden meer om vragen.

Self Assessments: Dichten van de 'kloof'

Om 'de kloof' te helpen dichten heeft IT Risk Control onder andere webbased self assessments ontwikkeld. In de assessments heeft IT Risk Control haar kennis, ervaringen en inzichten omgezet in handzame online vragenlijsten. Deze self assessments maken het mogelijk om snel, doeltreffend en gestructureerd informatie te verzamelen over de IT-omgeving en beheersmaatregelen bij cliënten.

Nadat het self assessment door de cliënt is ingevuld worden de resultaten door IT Risk Control geanalyseerd, verrijkt met relevante informatie en wordt een rapportage voor de accountant samengesteld. Daarmee kan de accountant direct inhoudelijk aan de slag. Onderstaande tabel geeft een overzicht van de assessments die in de accountantspraktijk worden ingezet.[6]

Naam assessment	Korte toelichting
General IT Assessment	Op basis van het algemeen COBIT normenkader geeft het assessment inzicht in de kwaliteit van de beheersmaatregelen die van primair belang zijn voor het waarborgen van de continuïteit en betrouwbaarheid van de geautomatiseerde gegevensverwerking. Het resultaat biedt gedegen input voor de managementletter. Tevens is voorzien in een verbeterplan voor de cliënt.
Administratieve Organisatie & Interne Beheersing	Dit assessment geeft inzicht in de sterke en zwakke punten bij uw cliënt. Het maakt de relaties zichtbaar tussen beheersmaatregelen in de bedrijfsprocessen, de systemen die daarbij worden gebruikt en relevante application controls. De uitkomsten helpen u te bepalen of een procesgerichte controle mogelijk is en welke tests zinvol zijn. De uitkomsten vormen een goede basis voor de managementletter.
IT Audit Essentials	Dit assessment is geschikt voor IT-omgevingen van klein tot groot. Het is een 'must have' als u snel en tegen lage kosten inzicht wil hebben in de IT-omgeving en essentiële beheersmaatregelen bij uw cliënt en informatie voor uw dossier. De uitkomsten bieden een gestructureerde basis om mogelijke risico's te bepalen en de aanpak van de controle hierop af te stemmen.

Tabel: Type assessments

[6] Voor informatie over deze assessments zie http://www.itriskcontrol.nl/onlineassessments/

Met de inzet van de assessments kan elk kantoor op een kosteneffectieve wijze een eerste stap zetten in het vergaren van relevante informatie en op professionele manier gestructureerd inzicht krijgen in mogelijke risico's en de controle aanpak en uitvoering daarop afstemmen en zo een begin te maken met het dichten van de 'kloof'.

General IT Assessment
Het General IT Assessment is gebaseerd op het breed erkend kader COBIT[7]. Op basis van dit raamwerk, zijn de beheersgebieden en beheersmaatregelen geïdentificeerd, die van primair belang zijn om de betrouwbare en continue werking van de geautomatiseerde gegevensverwerking te kunnen waarborgen. Het assessment vult de volgende behoefte van de accountant in:

- Inzicht in de IT organisatie en de IT systemen van de cliënt;
- Inzicht in de kwaliteit van de beheersmaatregelen;
- Ondersteuning keuze controle aanpak;
- Bieden van een basis voor een nadere gerichte toetsing van de maatregelen;
- Bijdrage aan dossiervorming.

Dit rapport
Dit rapport gaat over de ervaringen die wij hebben opgedaan met de inzet van de General IT Assessments. Dit betreft 190 assessments die wij in opdracht van accountantskantoren bij hun cliënten hebben uitgevoerd.

Met dit rapport willen wij kennis en inzichten delen. Wij willen vooral ook laten zien dat met zeer beperkte middelen toch een belangrijke behoefte van de accountant kan worden ingevuld. Niet alleen omdat het noodzakelijk is vanuit de (toenemende) vakinhoudelijke behoefte, maar vooral ook om de accountant in staat te stellen meer doelmatig te werken en meer toegevoegde waarde en onderscheidend vermogen aan cliënten te bieden. Dit is waar de cliënt vandaag de dag om vraagt. Wij spreken de verwachting uit met deze rapportage, vanuit ons vakgebied IT Audit, bij te dragen aan de ontwikkelingen in de accountancymarkt en de uitdagingen die daar liggen.
De rapportage bestaat uit twee delen, dit zijn:

Deel I : Beheersprocessen en beheersmaatregelen op basis van 190 assessments.
Deel II : Overzicht branches en sectoren en informatie over:

- De functiegebieden van automatisering;
- De pakketten die worden gebruikt;
- Aantal gebruikers per functiegebied;
- Standaard en maatwerk;
- Koppelingen.

IT Risk Control BV

[7] Zie www.isaca.org

I Beheerprocessen en beheersmaatregelen

Opzet en structuur General IT Assessment

Het doel van de inzet van het General IT Assessment in het kader van de accountantscontrole is inzicht te geven in de aard en kwaliteit van de beheersmaatregelen die door de organisatie zijn getroffen, om de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking te kunnen waarborgen.

In het assessment zijn vanuit COBIT de IT-processen opgenomen die relevant zijn in het kader van de accountantscontrole. Dit betreft de processen die direct in relatie staan tot de kwaliteitsaspecten: integriteit (juistheid en volledigheid), vertrouwelijkheid, beschikbaarheid en betrouwbaarheid van de geautomatiseerde gegevensverwerking en de daarvan afgeleide informatievoorziening en verslaglegging. Het betreft de volgende IT-processen:

- P01 Informatiestrategie;
- P09 Risicomanagement;
- AI6 Wijzigingenbeheer;
- DS4 Continuïteitsbeheer;
- DS5 Systeembeveiliging;
- DS11 Gegevensbeheer;
- DS12 Beheer fysieke IT-omgeving.

Voor het beoordelen van de niveaus van de IT-processen hanteert COBIT niveaus, op basis waarvan de volwassenheid van een proces kan worden geclassificeerd. Dit zijn:

- Niveau 0: Het proces is niet bestaand
- Niveau 1: Het proces is ongeorganiseerd/ad hoc
- Niveau 2: Het proces volgt een regelmatig patroon
- Niveau 3: Het proces is gedocumenteerd en gecommuniceerd
- Niveau 4: Het proces wordt gemanaged en is meetbaar
- Niveau 5: Best Practices worden toegepast

Het assessment is als volgt opgebouwd:

1) Op basis van een aantal algemene vragen, bijvoorbeeld ten aanzien van afhankelijkheid, complexiteit, aansluiting IT op de behoefte van de organisatie en dynamiek, wordt een typering van de automatiseringsomgeving bepaald. Deze typering[8] wordt gebruikt om een indicatie te hebben over de soort automatiseringsomgeving.
2) Voor elk van de bovengenoemde COBIT IT-processen wordt aan de organisatie gevraagd zichzelf in te schalen op een van de volwassenheidsniveaus;
3) Door middel van vervolgvragen over concrete beheersmaatregelen wordt vervolgens op basis van gesloten vragen (te beantwoorden met ja of nee) getoetst of het ingeschaalde niveau ook wordt bevestigd. Op basis hiervan ontstaat inzicht in het niveau van de processen en de mate waarin het aangegeven niveau wordt bevestigd door aangegeven beheersmaatregelen.

In het navolgende worden de uitkomsten voor elk IT beheerproces beschreven. Op basis van de uitkomsten van de 190 assessments kunnen veel (diepgaande) analyses worden uitgevoerd. Bijvoorbeeld naar branche, sector en/of pakket. Omdat dergelijke diepgaandere analyses niet bijdragen aan het doel van deze rapportage is ervoor gekozen om deze rapportage beperken tot de hoofdlijnen.

[8] Zie pagina 30 Typering automatiseringsomgeving

Vanwege de leesbaarheid en inzichtelijkheid is er verder voor gekozen een overwegend grafische presentatie en vaste structuur te hanteren. Deze structuur is als volgt:

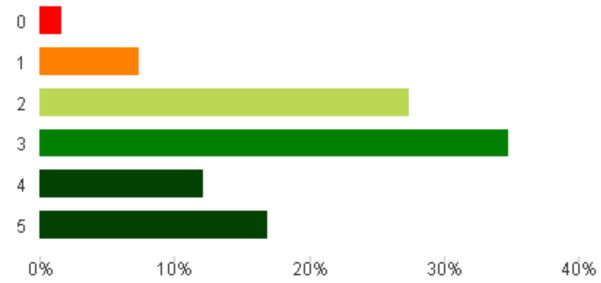
	Onderdeel	Toelichting
1	Aanduiding van het IT beheersproces	Code en naam vanuit COBIT
2	Korte beschrijving van het doel van het proces	Doelstelling volgens COBIT
3	Grafische presentatie van de aangegeven niveaus met een korte toelichting	Relatieve score op de niveaus 0 t/m 5
4	Grafische presentatie van de antwoorden op de onderliggende beheersmaatregelen.	Relatieve score van de Ja en Nee antwoorden. In het geval geen antwoord is gegeven wordt deze gerubriceerd als 'Niet Ingevuld'. Als een vraag niet is gesteld omdat niet wordt voldaan aan bovenliggende criteria wordt deze gerubriceerd als 'Niet gesteld'. Een voorbeeld van dit laatste. Als een cliënt aangeeft dat er geen continuïteitsplan is, worden vragen over het onderhouden van het continuïteitsplan in het assessment overgeslagen.
5	Analyse	Beknopte tekstuele analyse

P01 Informatiestrategie

Doel van Informatiestrategie
Voor een optimale benutting van de mogelijkheden dient de informatievoorziening te worden afgestemd op de bedrijfsbehoefte. Dit omvat onder andere het opstellen van regels over de betekenis en gebruik van gegevens(verzamelingen), gegevensclassificatie en beveiligingsniveaus. Het beheer van de informatievoorziening verbetert de kwaliteit van managementbeslissingen doordat de zekerheid over juist en betrouwbaar gebruik van informatie toeneemt.

Niveaus

Onderstaande grafiek toont de resultaten van het niveau waarop het proces Informatiestrategie is georganiseerd.



Niveaus Informatiestrategie

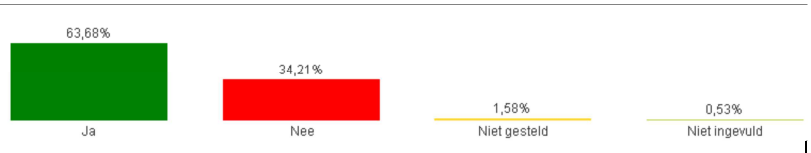
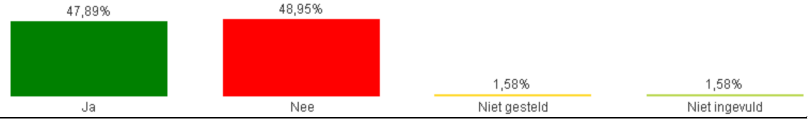
Legenda:

0: Proces is niet bestaand
1: Proces is ongeorganiseerd/ad hoc
2: Proces volgt een regelmatig patroon
3: Proces gedocumenteerd en gecommuniceerd
4: Proces gemanaged en meetbaar
5: Best Practices worden toegepast

Het merendeel van de organisaties geeft aan dat de informatiestrategie op niveau 3 of hoger is georganiseerd. 17 organisaties (9 %) geven aan in het geheel geen of alleen ad hoc aandacht te schenken aan het proces informatiestrategie.

Beheersmaatregelen

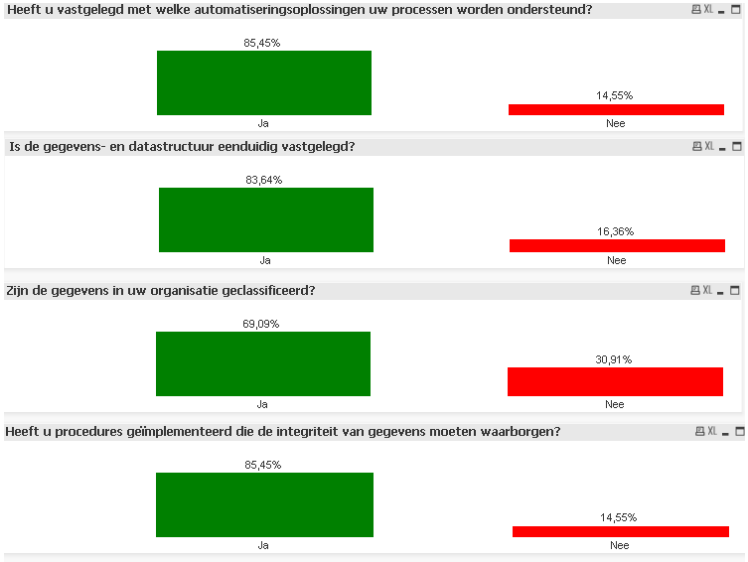
Om te toetsen of het aangegeven niveau 3 en hoger ook wordt daadwerkelijk wordt ondersteund door beheersmaatregelen zijn vervolgvragen gesteld. Onderstaande grafieken tonen per vraag de relatieve antwoorden.

Heeft u vastgelegd met welke automatiseringsoplossingen uw processen worden ondersteund?	
Is de gegevens- en datastructuur eenduidig vastgelegd?	
Zijn de gegevens in uw organisatie geclassificeerd?	
Heeft u procedures geïmplementeerd die de integriteit van gegevens moeten waarborgen?	

Uit een nadere analyse blijkt:

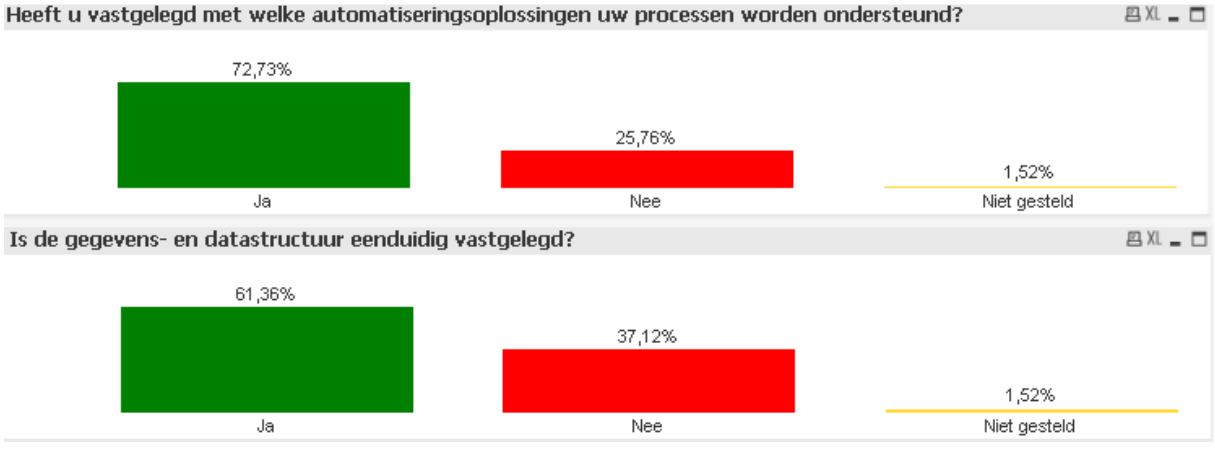
Bij het merendeel van de organisaties zijn de getroffen maatregelen in overeenstemming met het ingeschatte niveau.

55 organisaties (29%) geven aan Informatiemanagement op niveau 4 of 5 te hebben georganiseerd. Uit onderstaande grafieken blijkt echter dat deze organisaties voor een deel ontkennend moeten antwoorden op de onderliggende vragen. Zie onderstaande afbeelding:



Feitelijk voldoen deze organisaties dus niet aan de eisen die worden gesteld om het aangegeven niveau te kunnen rechtvaardigen.

Opvallend is verder dat organisaties die aangeven niet zonder automatisering te kunnen of daarvan sterk afhankelijk zijn, dit blijkbaar zonder vastgelegde strategie doen. Zie onderstaande afbeeldingen.



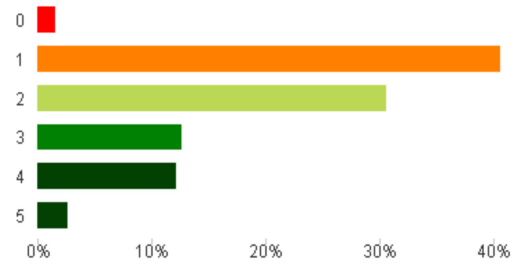
Grafiek: Organisaties die niet zonder automatisering kunnen en Informatiestrategie

P09 Risicomanagement

Doel risicomanagement
Risicobeheersing is gericht op het maken en onderhouden van een raamwerk voor beheersing van IT-risico´s. In een dergelijk raamwerk behelst het algemeen geaccepteerd risiconiveau, de strategie om risico's te beheersen en de geaccepteerde restrisico's te bepalen. Iedere mogelijke ongeplande gebeurtenis die een impact heeft op de doelstellingen van de organisatie zou moeten worden vastgesteld en moeten worden beoordeeld. De resultaten van de risicoanalyses dienen te worden gedocumenteerd op zodanige wijze dat deze begrepen kunnen worden door het management en belanghebbenden en gekwantificeerd kunnen worden afgewogen tegen de bedrijfsbelangen.

Niveaus

Onderstaande grafiek toont de resultaten van het niveau waarop het proces Risicomanagement is georganiseerd.



Niveaus Risicomanagement

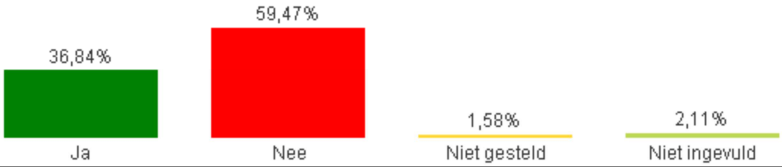
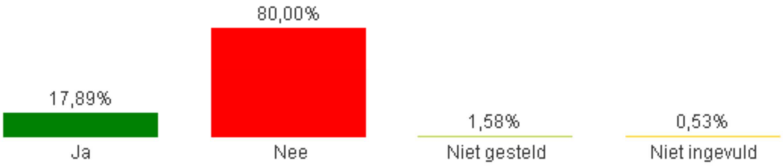
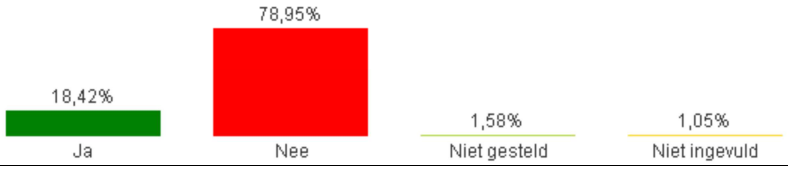
Legenda:

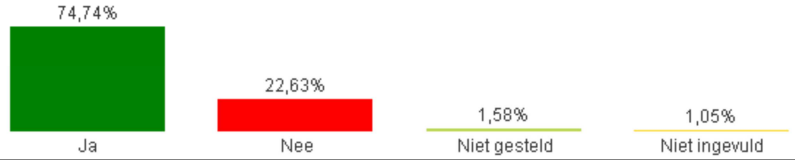
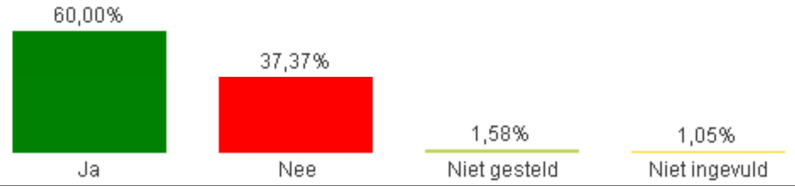
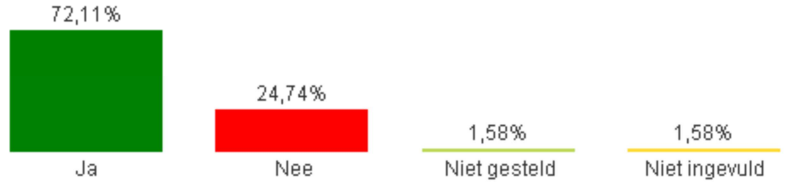
0: Proces is niet bestaand
1: Proces is ongeorganiseerd/ad hoc
2: Proces volgt een regelmatig patroon
3: Proces gedocumenteerd gecommuniceerd
4: Proces gemanaged en meetbaar
5: Best Practices worden toegepast

Het grootste deel van de ondernemingen heeft geen of slechts een rudimentair risicomanagement ingericht.

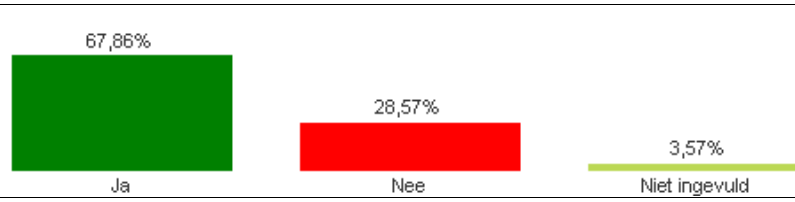
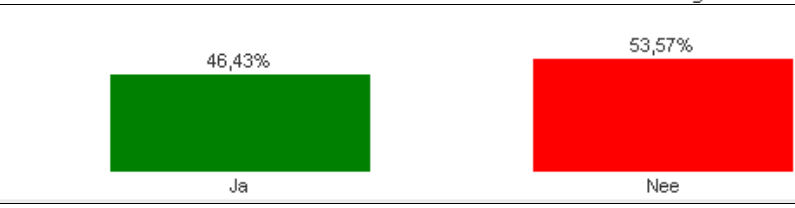
Beheersmaatregelen

Om te toetsen of het aangegeven niveau ook wordt behaald zijn vervolgvragen gesteld. Onderstaande grafieken tonen de relatieve antwoorden per vraag.

Is IT-risicobeheersing geïntegreerd met de beheersing van de bedrijfsrisico's?	
Beschikt u over een raamwerk voor risicoanalyse?	
Heeft u een risico-actieplan en wordt dit actueel onderhouden?	

Wordt bij het bepalen van de risico's rekening gehouden met de mogelijke impact van de gevolgen?	
Neemt u maatregelen tegen risico's en documenteert u deze?	
Beoordeelt u vastgestelde risico's naar waarschijnlijkheid en consequenties?	

28 Organisaties geven aan risicomanagement op het hoogste niveau te hebben georganiseerd. Uit nadere analyse blijkt echter dat deze organisaties voor een deel ontkennend moeten antwoorden op een aantal onderliggende vragen. Zie onderstaande afbeelding:

Is IT-risicobeheersing geïntegreerd met de beheersing van de bedrijfsrisico's?	
Beschikt u over een raamwerk voor risicoanalyse?	
Heeft u een risico-actieplan en wordt dit actueel onderhouden?	

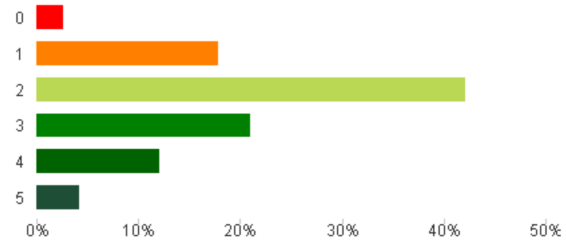
Feitelijk voldoen deze organisaties dus niet aan de eisen die worden gesteld om het aangegeven niveau te kunnen rechtvaardigen.

AI6 Wijzigingenbeheer

Doel Wijzigingenbeheer
Alle wijzigingen, inclusief noodmaatregelen en -patches, op de operationele infrastructuur en applicaties dienen beheerst te worden doorgevoerd. Beheerste doorvoering van wijzigingen betekent 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. Wijzigingsprocedures zorgen onder andere voor een uniforme afhandeling van wijzigingen op applicaties, procedures, processen en systemen.

Niveaus

Onderstaande grafiek toont de resultaten van het niveau waarop het proces Wijzigingenbeheer is georganiseerd.



Niveaus Wijzigingenbeheer

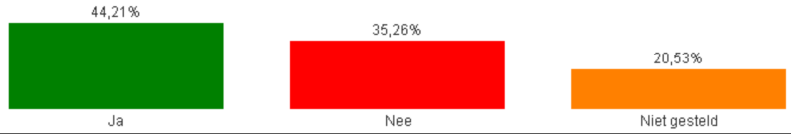
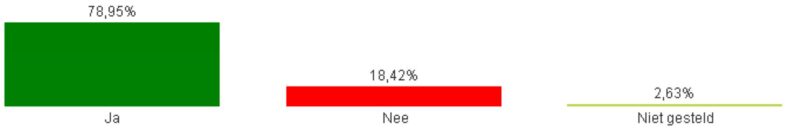
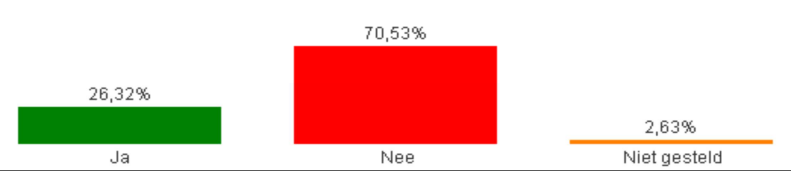
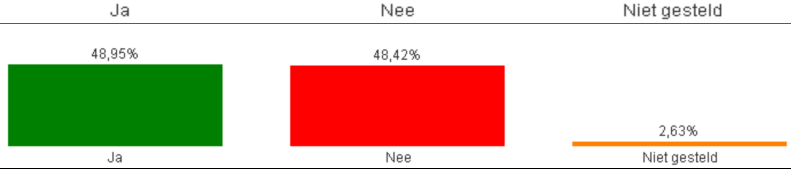
Legenda:

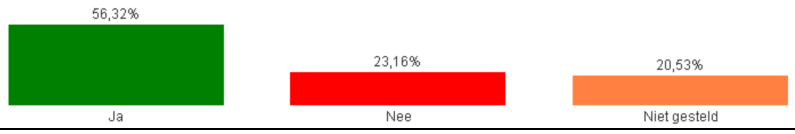
0: Proces is niet bestaand
1: Proces is ongeorganiseerd/ad hoc
2: Proces volgt een regelmatig patroon
3: Proces gedocumenteerd gecommuniceerd
4: Proces gemanaged en meetbaar
5: Best Practices worden toegepast

39 organisaties (21 %) geven aan Wijzigingsbeheer niet of ad hoc in te vullen. 80 organisaties (42 %) geeft aan dat Wijzigingsbeheer een regelmatig patroon volgt.

Beheersmaatregelen

Om te toetsen of het aangegeven niveau ook wordt behaald zijn vervolgvragen gesteld. Onderstaande grafieken tonen de relatieve antwoorden per vraag.

Heeft u procedures voor wijzigingenbeheer vastgesteld?	
Worden wijzigingen beoordeeld op impact, prioriteit en noodzakelijke goedkeuring voordat deze worden doorgevoerd?	
Zijn voor spoedwijzigingen procedures aanwezig?	
Worden status en resultaten van wijzigingen gerapporteerd?	

Worden wijzigingen gedocumenteerd en wordt de systeemdocumentatie ook aangepast?	

Uit een nadere analyse komt onder andere naar voren:

71 organisaties (37 %) geven aan het wijzigingsbeheer op niveau 3 of hoger te hebben georganiseerd. Van deze organisaties heeft 48 % echter geen procedures ingericht voor spoedwijzigingen. Dergelijke wijzigingen vereisen speciale aandacht en procedures om achteraf alsnog de spoedwijziging te kunnen beoordelen en eventueel te kunnen corrigeren.

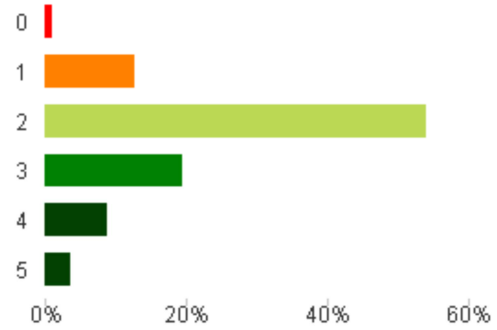
DS4 Continuïteitsbeheer

Doel continuïteitsbeheer

Het waarborgen van de continue beschikbaarheid van de IT-voorzieningen vereist het ontwikkelen, onderhouden en testen van continuïteitsplannen, het opslaan van back-up op een externe locatie en het periodiek trainen op de werking van de plannen.

Niveaus

Onderstaande grafiek toont de resultaten van het niveau waarop het proces Continuïteitsbeheer is georganiseerd.



Legenda:

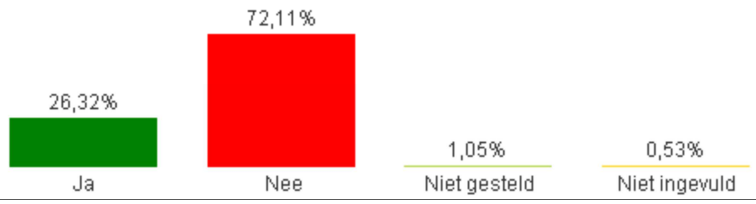
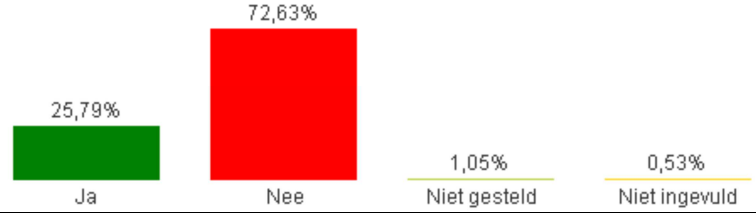
0: Proces is niet bestaand
1: Proces is ongeorganiseerd/ad hoc
2: Proces volgt een regelmatig patroon
3: Proces gedocumenteerd gecommuniceerd
4: Proces gemanaged en meetbaar
5: Best Practices worden toegepast

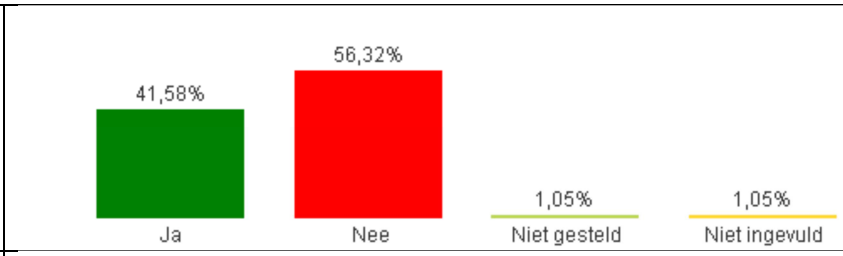
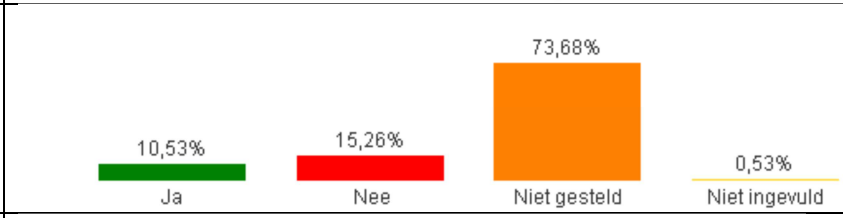
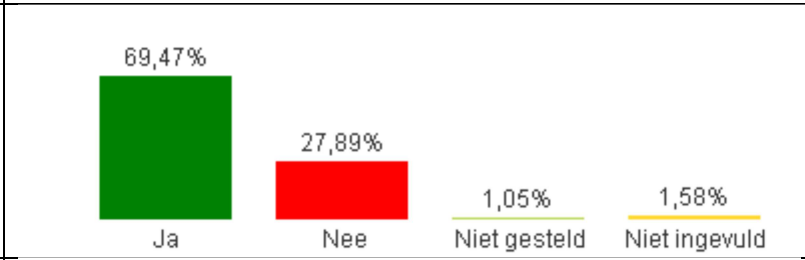
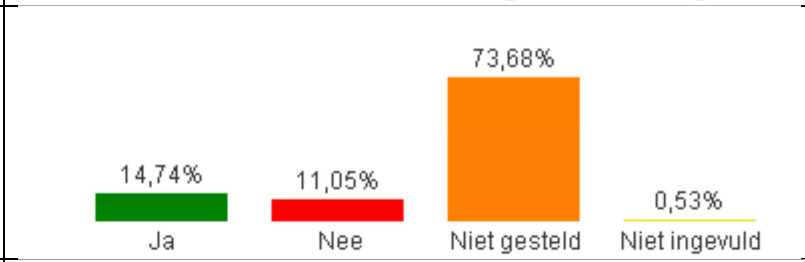
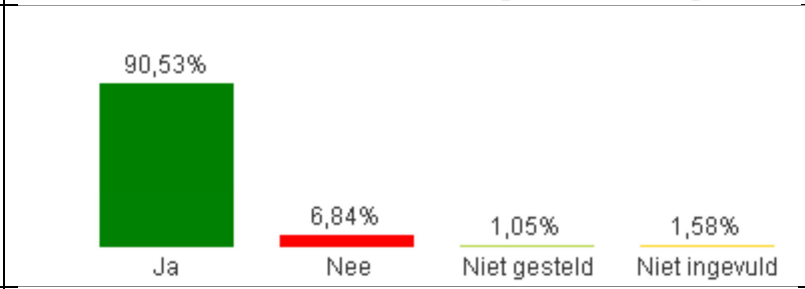
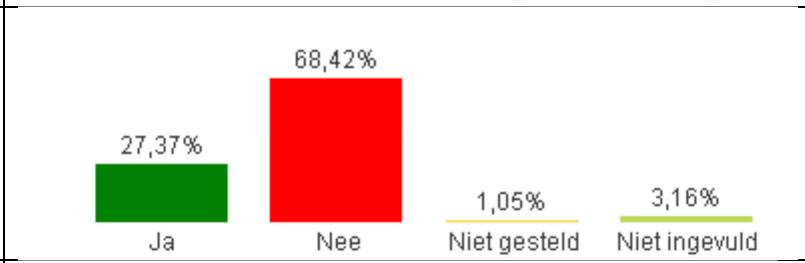
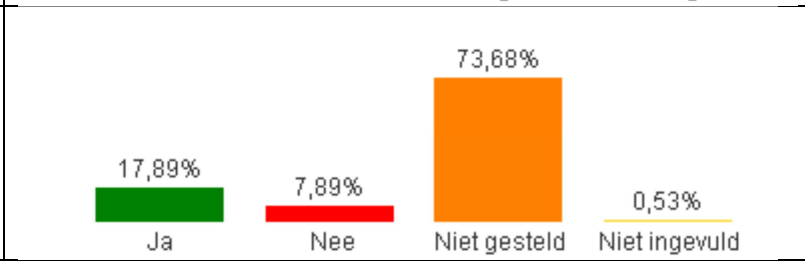
Niveaus continuïteitsbeheer

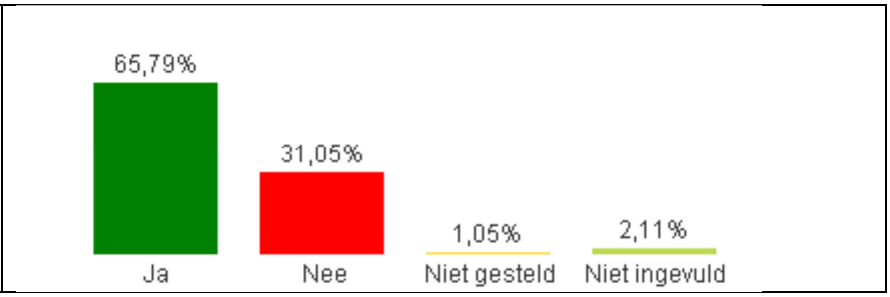
26 organisaties (14 %) geven aan continuïteitsbeheer niet en/of ad hoc in te vullen. Het merendeel 103 (54 %) geeft aan dat het continuïteitsproces een regelmatig patroon volgt. Tegelijk betekent dit dat het continuïteitsproces bij het merendeel (68 %) niet is gedocumenteerd en gecommuniceerd. Hier ligt dus een belangrijk aandachtspunt.

Beheersmaatregelen

Om te toetsen of het aangegeven niveau ook wordt behaald zijn vervolgvragen gesteld. Onderstaande grafieken tonen de relatieve antwoorden per vraag.

Past u een raamwerk voor continuïteitsbeheer toe?	
Zijn continuïteitsplannen opgesteld?	

Is er een planning voor de volgorde van herstel van de IT-activiteiten na een calamiteit?	
Wordt het continuïteitsplan jaarlijks getest?	
Zijn kritische IT-middelen en personen vastgesteld?	
Is het continuïteitsplan verspreid onder alle betrokkenen?	
Worden back-ups ook op een externe locatie opgeslagen?	
Worden alle betrokkenen getraind in de procedures ten aanzien van continuïteit?	
Wordt het continuïteitsplan jaarlijks onderhouden?	

Worden herstelactiviteiten na een storing altijd geëvalueerd?	

Uit een nadere analyse komt onder andere naar voren:

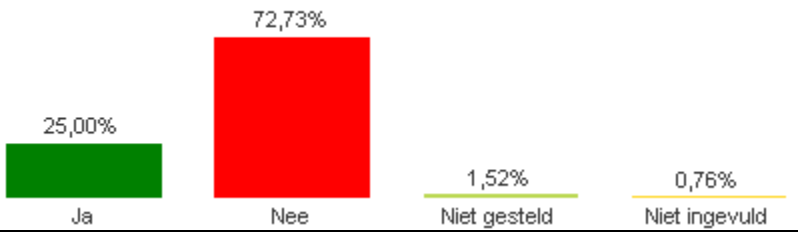
Van de 164 organisaties die aangeven het proces op niveau 2 of hoger te hebben georganiseerd maar 47 organisaties (29%) aangeven te beschikken over een continuïteitsplan.

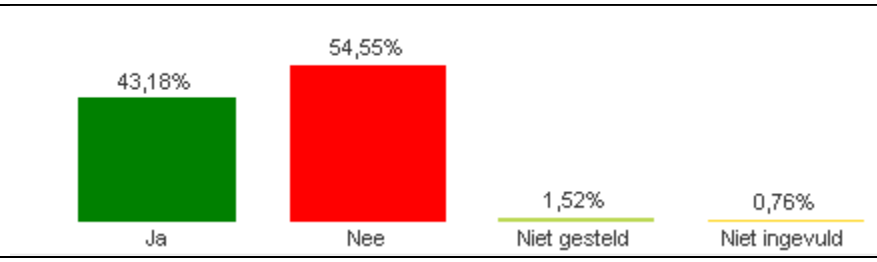
117 organisatie (71 %) beschikken dus niet over een continuïteitsplan. Het continuïteitsplan minimaliseert de impact van een grote verstoring in de IT-voorzieningen op de bedrijf kritische processen en IT-systemen. In het plan is onder andere opgenomen welke alternatieven voorhanden zijn, wat de kritische IT-diensten zijn en welke procedures worden gevolgd.

Van de 47 organisaties die wel beschikken over een continuïteitplan geeft 43 % aan dat het plan jaarlijks wordt getest. 57 % van de organisaties beschikt dus wel over een plan, maar heeft geen zekerheid dat dit werkt en blijft werken. Regelmatig testen van het plan maakt het mogelijk om tijdig tekortkomingen te signaleren en de plannen hierop aan te passen, zodat steeds kan worden beschikt over een werkend plan.

Verder komt naar voren dat 6,8 % van de organisaties de back-up niet extern opslaat. Opslag van belangrijke back-upmedia, documentatie en andere IT-hulpmiddelen op een externe locatie waarborgt de beschikbaarheid van bedrijf kritische middelen en -gegevens.

Opvallend is verder dat organisaties die aangeven niet zonder automatisering te kunnen of sterk afhankelijk zijn, dit niet laten doorwerken in hun continuïteitsmaatregelen. Zie onderstaande grafieken.

Past u een raamwerk voor continuïteitsbeheer toe?	
Zijn continuïteitsplannen opgesteld?	

Is er een planning voor de volgorde van herstel van de IT-activiteiten na een calamiteit?	

Grafiek: Organisaties die niet zonder automatisering kunnen en continuïteit

DS5 Systeembeveiliging

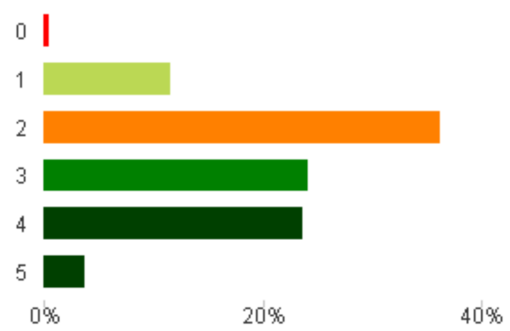
Doel Systeembeveiliging

De noodzaak om de integriteit van informatie te waarborgen en de IT-middelen te beschermen maakt een proces van systeembeveiliging noodzakelijk. Dit omvat het vaststellen en onderhouden van IT-beveiligingsrollen en -verantwoordelijkheden, beveiligingsbeleid, standaarden en procedures. Het betreft ook het monitoren van informatiebeveiliging en de periodieke toetsing en implementatie van correctieve maatregelen indien zwakheden in de beveiliging zijn aangetroffen of beveiligingsincidenten zich hebben voorgedaan. Effectieve systeembeveiliging beschermt alle IT-middelen zodat het risico van impact van beveiligingsincidenten op de bedrijfsprocessen wordt geminimaliseerd.

Niveaus

Onderstaande grafiek toont de resultaten van het niveau waarop het proces Systeembeveiliging is georganiseerd.

Systeembeveiliging



Legenda:

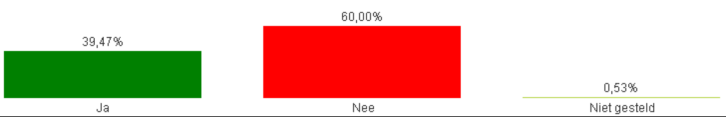
0: Proces is niet bestaand
1: Proces is ongeorganiseerd/ad hoc
2: Proces volgt een regelmatig patroon
3: Proces gedocumenteerd gecommuniceerd
4: Proces gemanaged en meetbaar
5: Best Practices worden toegepast

Niveaus Systeembeveiliging

23 organisaties (12 %) geven aan Systeembeveiliging niet en/of ad hoc in te vullen. 69 organisaties (36 %) geven aan dat het proces van systeembeveiliging een regelmatig patroon volgt (niveau 2). Dit betekent dus dat het merendeel van de organisaties (92 organisaties, 48 %) niet beschikt over een gedocumenteerd en gecommuniceerd proces van systeembeveiliging. Hier ligt dus een belangrijk aandachtspunt.

Beheersmaatregelen

Aan de organisaties die zichzelf hebben ingeschaald op niveau 2 of hoger zijn vervolgvragen gesteld. Onderstaande grafieken tonen de relatieve antwoorden per vraag.

Is informatiebeveiliging benoemd in de portefeuilles van het topmanagement?	
Is een informatiebeveiligingsplan opgesteld?	

Zijn procedures opgesteld voor gebruikersbeheer?	
Wordt minimaal jaarlijks de informatiebeveiliging getest en beoordeeld?	
Zijn maatregelen getroffen ter voorkoming, herkenning en correctie van schadelijke software?	
Zijn procedures opgesteld voor gegevensuitwisseling van gevoelige informatie?	
Zijn procedures opgesteld voor de identificatie en afhandeling van beveiligingsincidenten?	
Zijn procedures opgesteld voor de bescherming van hulpmiddelen die gebruikt worden voor informatiebeveiliging	
Zijn procedures opgesteld voor beheer van cryptografische sleutels?	
Zijn procedures opgesteld voor beheer van gebruikersrechten?	
Zijn maatregelen getroffen ten aanzien van netwerkbeveiliging?	

Uit een nadere analyse komt onder andere naar voren:

Van de 167 organisaties die aangeven het proces op niveau 2 of hoger te hebben georganiseerd voert 56 % jaarlijks geen beoordeling en/of testen uit op de informatiebeveiliging. Regelmatig testen en beoordelen van de bestaande maatregelen van informatiebeveiliging waarborgt het niveau van beveiliging en het vasthouden hiervan. Hierdoor kan zekerheid worden verkregen dat belangrijke risico's daadwerkelijk zijn afgedekt. Bij de betrokken organisaties bestaat daarom de kans dus dat sprake is van schijnzekerheid. Om deze reden en het toenemend aantal bedreigingen is het van belang periodiek de beveiliging te testen.

Bij het merendeel van deze 167 organisaties zijn geen procedures opgesteld voor de identificatie en afhandeling van beveiligingsincidenten. Beveiligingsincidenten zouden als zodanig herkenbaar moeten zijn en moeten worden geregistreerd. Dit maakt het mogelijk adequate en duurzame maatregelen te treffen.

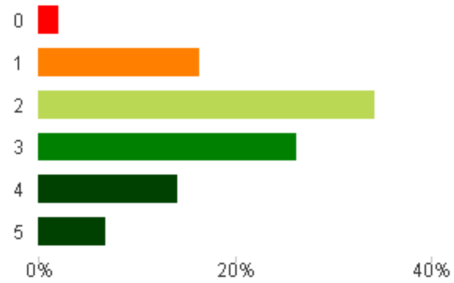
DS11 Gegevensbeheer

Doel Gegevensbeheer

Voor een effectief gegevensbeheer is het nodig vast te stellen waaraan gegevens moeten voldoen. Het proces gegevensbeheer omvat tevens procedures voor effectief beheer van de data, back-up en recovery van gegevens, en een juiste en veilige vernietiging van gegevens. Gegevensbeheer draagt bij aan de kwaliteit, tijdigheid en beschikbaarheid van bedrijfsgegevens.

Niveaus

Onderstaande grafiek toont de resultaten van het niveau waarop het proces Gegevensbeheer is georganiseerd.



Niveaus Gegevensbeheer

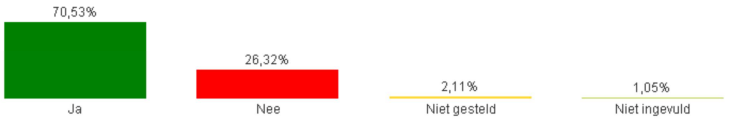
Legenda:

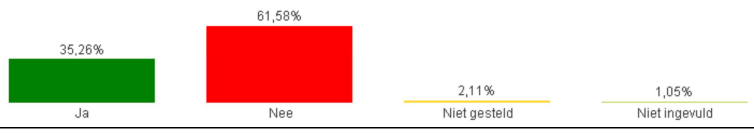
0: Proces is niet bestaand
1: Proces is ongeorganiseerd/ad hoc
2: Proces volgt een regelmatig patroon
3: Proces gedocumenteerd gecommuniceerd
4: Proces gemanaged en meetbaar
5: Best Practices worden toegepast

23 organisaties (12 %) geven aan Gegevensbeheer niet en/of ad hoc in te vullen. 58 (31 %) geeft aan dat Gegevensbeheer een regelmatig patroon volgt.

Beheersmaatregelen

Om te toetsen of het aangegeven niveau ook wordt behaald zijn vervolgvragen gesteld. Onderstaande grafieken tonen de relatieve antwoorden per vraag.

Zijn eisen ten aanzien van gegevensbeheer opgesteld vanuit het belang van de bedrijfsprocessen?	
Zijn procedures aanwezig voor opslag en archivering van gegevens?	
Zijn back-up en herstelprocedures van systemen en gegevens aanwezig?	
Zijn procedures aanwezig voor beheer van media voor gegevensopslag?	

Zijn procedures aanwezig voor vernietiging van media en gegevens?	
Zijn maatregelen getroffen om de noodzaak van bescherming van gegevens te waarborgen?	

Uit een nadere analyse komt onder andere naar voren:

90 organisaties geven aan dat het Gegevensbeheer op niveau 3 of hoger te hebben georganiseerd. Eén van de maatregelen is bijvoorbeeld het voorkomen van ongeoorloofde toegang tot gevoelige informatie en software welke vernietigd gaat worden, bijvoorbeeld door opslag in beveiligde containers voor vernietiging.
56 % van deze bedrijven beschikt echter niet over processen voor de vernietiging van media en gegevensdragers.

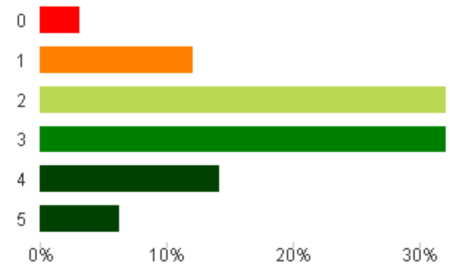
DS12 Fysieke beveiliging

Doel Fysieke beveiliging
Voor de bescherming van computerapparatuur en IT-personeel zijn goede fysieke voorzieningen nodig. Het proces van beheersing van de fysieke omgeving omvat tevens het vaststellen van vereisten aan de fysieke locatie, de selectie van de juiste voorzieningen en de mogelijkheden om de omgevingsfactoren en toegang tot de ruimtes te monitoren en te beperken. Effectieve beheersing van de fysieke omgeving van IT-voorzieningen minimaliseert verstoringen van de geautomatiseerde gegevensverwerking.

29 organisaties (15 %) geven aan Fysieke beveiliging niet en/of ad hoc in te vullen. 61 organisaties (32 %) geeft aan dat Fysieke beveiliging een regelmatig patroon volgt.

Niveaus

Onderstaande grafiek toont de resultaten van het niveau waarop het proces Fysieke beveiliging is georganiseerd.



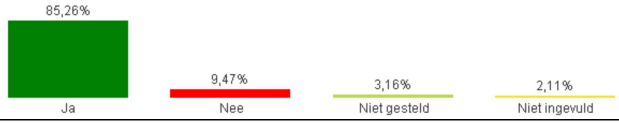
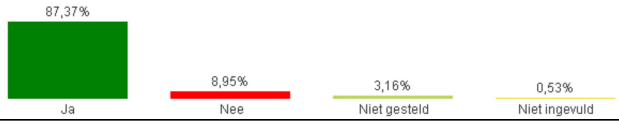
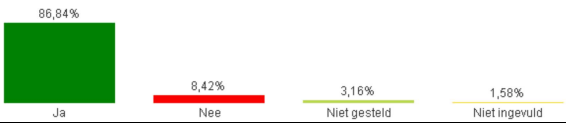
Niveaus Fysieke beveiliging

Legenda:

0: Proces is niet bestaand
1: Proces is ongeorganiseerd/ad hoc
2: Proces volgt een regelmatig patroon
3: Proces gedocumenteerd gecommuniceerd
4: Proces gemanaged en meetbaar
5: Best Practices worden toegepast

Beheersmaatregelen

Om te toetsen of het aangegeven niveau ook wordt behaald zijn vervolgvragen gesteld. Onderstaande grafieken tonen de relatieve antwoorden per vraag.

Is de bepaling van locatie en indeling van serverruimte(s) zorgvuldig uitgevoerd?	
Zijn voldoende fysieke beveiligingsmaatregelen getroffen?	
Wordt de fysieke toegang beheerst?	
Zijn beschermende maatregelen getroffen tegen omgevingsfactoren?	

Zijn voldoende maatregelen getroffen voor adequaat beheer van de fysieke ruimtes?	

Uit de resultaten kan worden afgeleid dat de maatregelen met betrekking tot de fysieke beveiliging in lijn zijn met de aangegeven niveaus.

II Sectoren, branches, typering en software omgeving

Branches/sectoren

Dit rapport is gebaseerd op de uitkomsten van de assessments van 190 organisaties die actief zijn in 32 branches/sectoren. Zie onderstaande tabel.

Branche	# Organisaties	Fte's	Werkplekken
01 Landbouw, jacht en dienstverlening voor de landbouw en jacht	4	157	90
05 Visserij, kweken van vis en schaaldieren	3	618	186
15 Vervaardiging van voedingsmiddelen en dranken	5	50	10
16 Verwerking van tabak	1	440	170
21 Vervaardiging van papier, karton en papier- en kartonwaren	3	4020	1742
22 Uitgeverijen, drukkerijen en reproductie van opgenomen media	3	495	311
24 Vervaardiging van chemische producten	2	2764	1787
27 Vervaardiging van metalen in primaire vorm	1	1776	877
28 Vervaardiging van producten van metaal (geen machines en transportmiddelen)	7	3750	4117
29 Vervaardiging van machines en apparaten	5	481	821
31 Vervaardiging van overige elektrische machines, apparaten en benodigdheden	4	601	340
32 Vervaardiging van audio-, video- en telecommunicatieapparaten en -benodigdheden	1	508	554
34 Vervaardiging van auto's, aanhangwagens en opleggers	1	140	100
35 Vervaardiging van transportmiddelen (geen auto's, aanhangwagens en opleggers)	1	1339	1212
45 Bouwnijverheid	27	200	50
50 Handel in en reparatie van auto's en motorfietsen; benzineservicestations	7	565	353
51 Groothandel en handelsbemiddeling (niet in auto's en motorfietsen)	37	3525	327
52 Detailhandel en reparatie consumentenartikelen (geen auto's, motors en brandstoffen)	5	30	17
60 Vervoer over land	12	165	114
61 Vervoer over water	1	105	50
63 Dienstverlening voor het vervoer	1	830	384
65 Financiële instellingen (uitgezonderd verzekeringswezen en pensioenfondsen)	5	115	50
67 Fin. beurzen, eff makelaars, assurantiepersonen, adm.kant. tbv aandelen, waarborgfondsen e.d.	2	77	80
71 Verhuur transportmiddelen, machines en werktuigen en overige roerende goederen	1	132	374
72 Computerservice en informatietechnologie	10	250	305
74 Overige zakelijke dienstverlening	20	50	50
75 Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen	2	115	80
80 Onderwijs	1	236	300
85 Gezondheids- en welzijnszorg	4	85	50
91 Werkgevers-, werknemers- en beroepsorg. politieke org. en overige ideële org.	1	25	30
92 Cultuur, sport en recreatie	1	550	2000**
93 Overige dienstverlening	12	55	12
	190	**24249**	**16943**

Tabel: Organisaties, Fte's en werkplekken.

*Door een van de organisatie is in plaats van het aantal organieke Fte's het aantal Fte's opgegeven dat belast is met automatisering. **In de werkplekken zijn ook de werkplekken van de leerlingen betrokken, deze zijn niet in begrepen in het aantal Fte's.

Typering automatiseringsomgeving

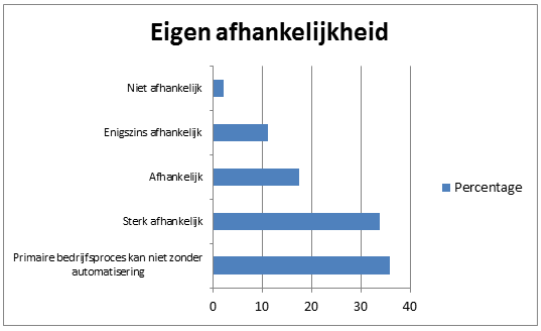
In het assessment zijn een aantal typeringsvragen opgenomen. Het belangrijkste doel van de typeringsvragen is, om bij de beoordeling van de risico's en het geven van aanbevelingen niet zonder meer voor elke organisatie dezelfde meetlat te gebruiken, zonder daarbij rekening te houden met de specifieke situatie**.**

Onderstaand een overzicht van een aantal vragen, dat voor de typering wordt gebruikt.
Deze zijn in deze rapportage opgenomen om een beeld te geven over de uiteenlopende typeringen automatiseringsomgevingen die in de basis al bestaan.

Daarbij wordt volstaan met het geven van de percentages van de antwoorden. Een verdere analyse is niet in deze rapportage opgenomen.

Eigen afhankelijkheid

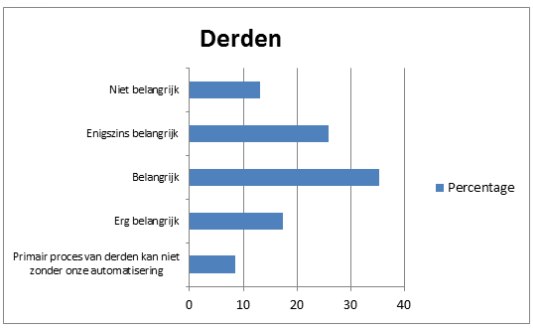
Met deze vraag wordt nagegaan in hoeverre de eigen organisatie afhankelijk is van de beschikbaarheid van de automatisering. Dit kan een indicatie zijn dat aan de eisen met betrekking tot continuïteit hoge eisen moeten worden gesteld. Onderstaande grafiek toont de percentages van de antwoorden.



Grafiek: Eigen afhankelijkheid

Afhankelijkheid voor derden

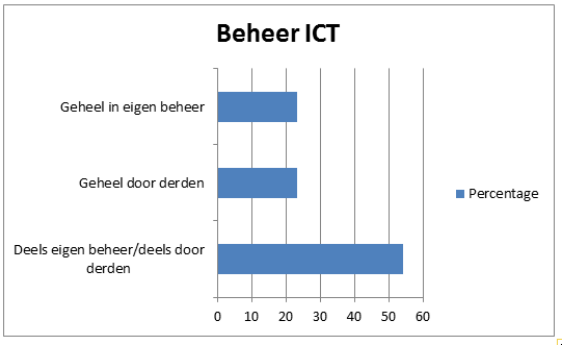
Met deze vraag wordt nagegaan in hoeverre de beschikbaarheid van de automatisering van belang is voor derden waarmee de organisatie zaken doet. Dit kan een indicatie geven dat aan de eisen met betrekking tot continuïteit specifieke eisen worden gesteld, bijvoorbeeld voor het kunnen waarborgen van de leverbetrouwbaarheid. Onderstaande grafiek toont de percentages van de antwoorden.



Grafiek: Eigen afhankelijkheid derden

Beheer ICT

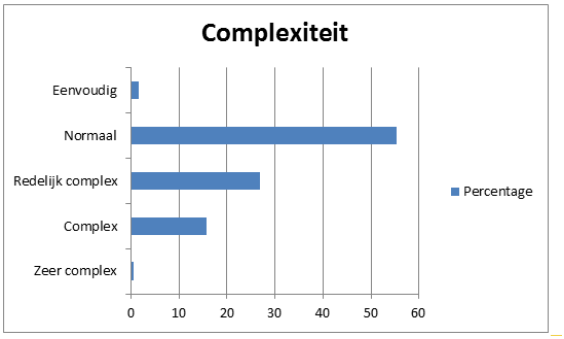
Met deze vraag wordt nagegaan door wie het beheer wordt gevoerd. Dit kan een indicatie geven voor de afhankelijkheid van derden en het belang om aandacht te schenken aan de afspraken die daarover zijn gemaakt, bijvoorbeeld SLA's. Onderstaande grafiek toont de percentages van de antwoorden.



Grafiek: Beheer ICT

Complexiteit

Deze vraag is erop gericht inzicht te krijgen in de complexiteit van de automatiseringsomgeving. Hoe complexer de omgeving des te meer eisen worden gesteld aan de kwaliteit van de beheersmaatregelen. Onderstaande grafiek toont de percentages van de antwoorden.



Grafiek: Complexiteit

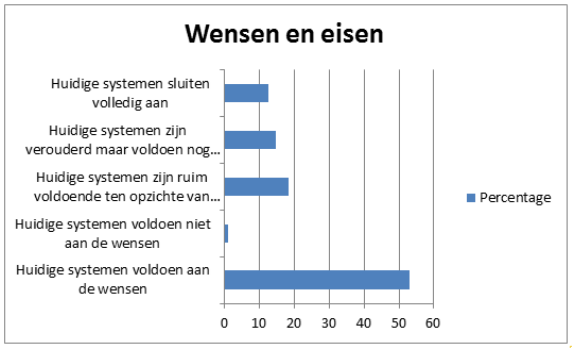
Betrokkenheid van het management

De betrokkenheid van het management is van groot belang om de IT-oplossingen zo goed mogelijk aan te kunnen laten sluiten aan de bedrijfsbehoefte Onderstaande grafiek toont de percentages van de antwoorden.

Grafiek: Betrokkenheid management

Aansluiting behoefte

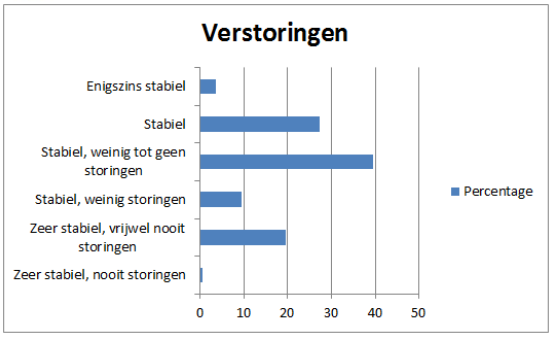
Als systemen niet aansluiten bestaat het risico op het ontstaan van alternatieve registraties en subsystemen. Deze zijn vaak minder goed beheersbaar en onttrekken zich aan het waarnemend oog. Tevens bestaat hierdoor de kans op sub optimalisatie, zonder dat het management daar wellicht kennis van heeft. Onderstaande grafiek toont de percentages van de antwoorden.



Grafiek: Wensen en eisen

Verstoringen

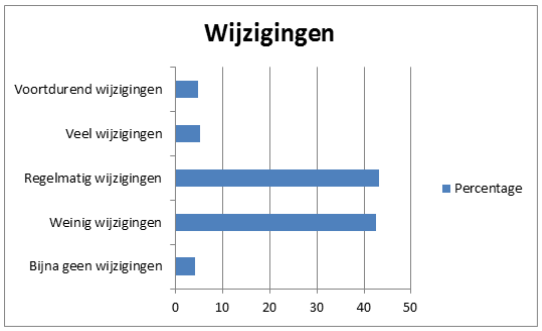
Verstoringen in de geautomatiseerde gegevensverwerking kunnen verstrekkende gevolgen hebben. Zeker als de organisatie of derden in belangrijk mate afhankelijk zijn van de automatisering. Deze vraag is erop gericht inzicht te krijgen in de storingsgevoeligheid van de automatiseringsomgeving. Onderstaande grafiek toont de percentages van de antwoorden.



Grafiek: Verstoringen

Wijzigingen

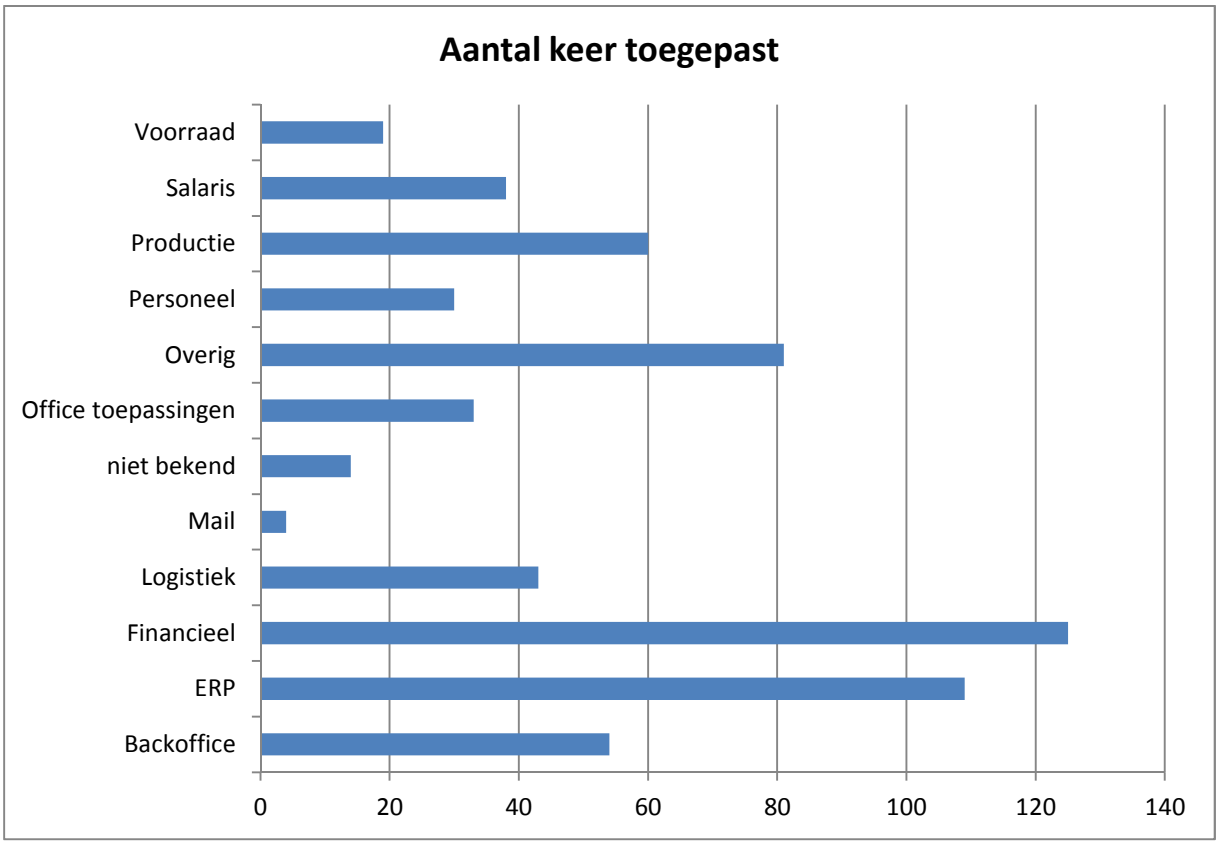
Wijzigingen in de systemen kunnen de werking verstoren. In omgevingen waar de dynamiek van wijzigingen hoog is, bijvoorbeeld als gevolg van wijzigingen in de behoefte van de markt en/of eigen organisatie moeten hogere eisen worden gesteld aan het proces van wijzigingen beheer. Onderstaande grafiek toont de percentages van de antwoorden.



Grafiek: Wijzigingen

Pakketten en gebruikers

In de assessments wordt gevraagd aan te geven welke vijf (5) pakketten voor de organisatie het meest belangrijk zijn. In totaal worden daarbij 610 pakketten genoemd. Na ontdubbeling blijkt dat het gaat om 367 verschillende pakketten. De navolgende grafieken geven inzicht in enkele waarnemingen:



Grafiek: Pakketten naar functiegebied[9]

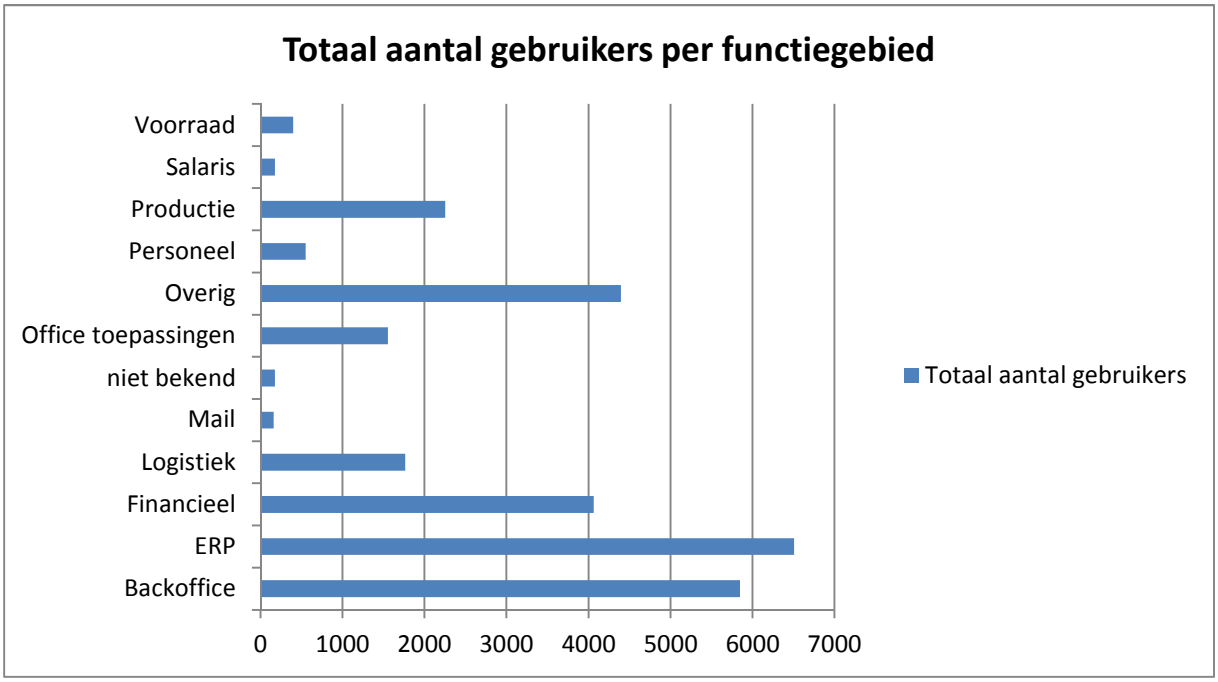
Vanzelfsprekend worden een aantal pakketten vaker worden genoemd dan andere pakketten. Dit betreft pakketten van Microsoft (Navision /Axapta) en Exact (Exact, Globe, Financials). Wat betreft het aantal keren dat deze pakketten worden genoemd is er nagenoeg geen verschil. Microsoft en Exact worden elk in ca. 8 % van de gevallen genoemd.

Het aantal van 367 maakt echter ook duidelijk dat er een scala aan uiteenlopende pakketten is. Deze grote mate van diversiteit brengt de uitdaging mee zich mee om ten aanzien van diverse pakketten kennis te verwerven en te behouden.

Uit de grafiek komt verder onder andere naar voren dat de pakketten in de functiegebieden Financieel, ERP en productie als het meest belangrijk worden aangemerkt. Dit ligt voor de hand omdat deze functiegebieden de kern van de bedrijfsprocessen raken.

In het functiegebied overige worden onder andere pakketten genoemd voor Customer Relation Management (CRM), Business Intelligence, CAD/CAM, Documentatie/informatiesystemen. Het is voorstelbaar dat afhankelijk van de kernactiviteiten van een organisatie dergelijke systemen als belangrijkste pakketten worden aangemerkt.

[9] Organisaties hanteren niet altijd dezelfde functionele aanduiding voor een pakket. Deels heeft dit te maken met overlappende functionaliteit van pakketten (ERP omvat ook financieel, productie en voorraad).



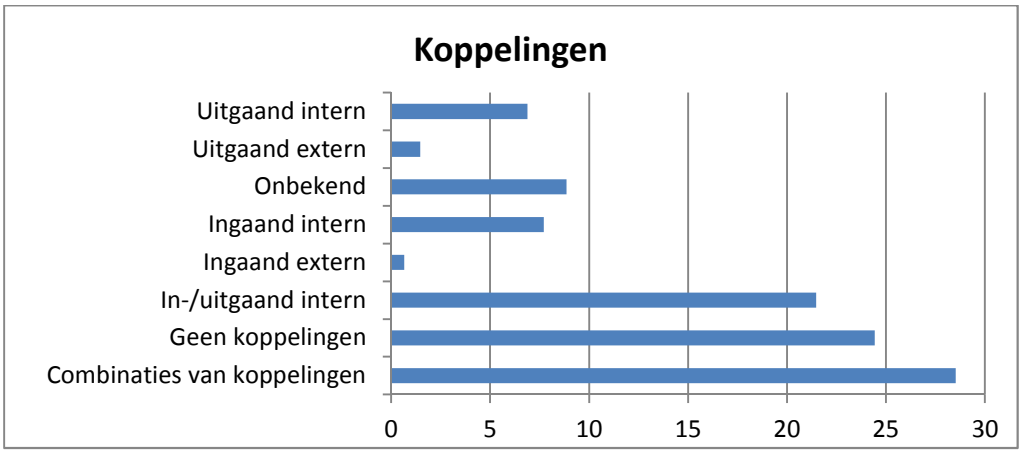
Grafiek: Pakketten naar Totaal aantal gebruikers

De functiegebieden ERP, Backoffice, Financieel en Overig hebben het grootst aantal gebruikers. Gelet op de overwegend bedrijfsbrede(re) inzet ligt dit voor de hand.

Koppelingen

Een belangrijk kenmerk van ERP systemen is de verregaande mate van integratie tussen de verschillende functiegebieden. Handelingen, zoals inkooporders, voorraadbewegingen, productie en verkopen worden daarbij direct vertaald naar transacties in het grootboek en andere relevante onderdelen van het ERP-pakket. De verwerkingsmechanismen die hiervoor in het ERP systeem zijn opgenomen bieden veelal voldoende waarborgen om de betrouwbare verwerking te kunnen waarborgen en controle daarop uit te kunnen oefenen. Uiteraard moeten deze mechanismen dan wel goed zijn ingeregeld en worden beheerst.

Maar ook bij 'standalone' pakketten is er behoefte aan een geautomatiseerde uitwisseling van gegevens tussen de pakketten. Dubbel invoeren is immers niet efficiënt en de kans op fouten is groot. Het realiseren van koppelingen is meestal maatwerk. Hoewel er andere technologieën beschikbaar zijn, zijn koppelingen veelal nog gebaseerd op het aanmaken van exportdata vanuit het bronsysteem en het importeren van de exportdata in het doelsysteem. Omdat de keten zo sterk is als de zwakte schakel wordt in het assessment ook gevraagd naar de aanwezigheid van koppelingen. De navolgende grafiek toont de resultaten.



Grafiek: Koppelingen

Uit de grafiek kan onder andere worden opgemaakt dat in het merendeel van gevallen er sprake is van koppelingen tussen de pakketten. Slechts in 25 % van de pakketten is er geen sprake van een koppeling.

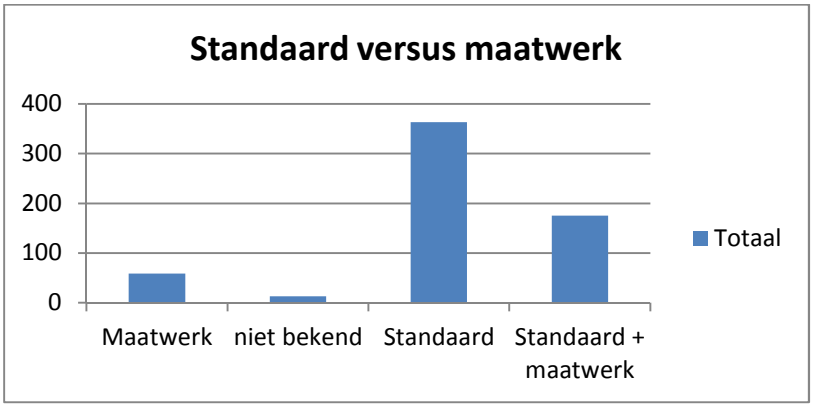
Gelet op de verhoogde risico's liggen hier belangrijke aandachtspunten[10] voor de controle.

Maatwerk of standaard

Een standaardpakket heeft voordelen. Bijvoorbeeld in relatie tot de onderhoudbaarheid, het proces van changemanagement en de kosten van de software. Een nadeel kan zijn dat de organisatie zich moet aanpassen aan de beschikbare standaard functionaliteit. Mits een geschikt pakket is gekozen hoeft dit echter geen bezwaar te zijn. 'Waarom zou een organisatie geheel anders zijn dan de rest van de branchegenoten?'

In een aantal gevallen is een standaardpakket echter niet toereikend. In dat geval is men aangewezen op aanpassingen van het standaard pakket of zelfs geheel maatwerk. Vanwege onder andere het belang voor het proces van changemanagement als onderdeel van de General IT Controls wordt daarom in het assessment gevraagd naar de aard van de software.

De navolgende grafiek toont de resultaten.



Grafiek: Standaard versus maatwerk

[10] http://www.itriskcontrol.nl/qa/interfaces/wat-zijn-belangrijke-aandachtspunten-bij-interfaces.html

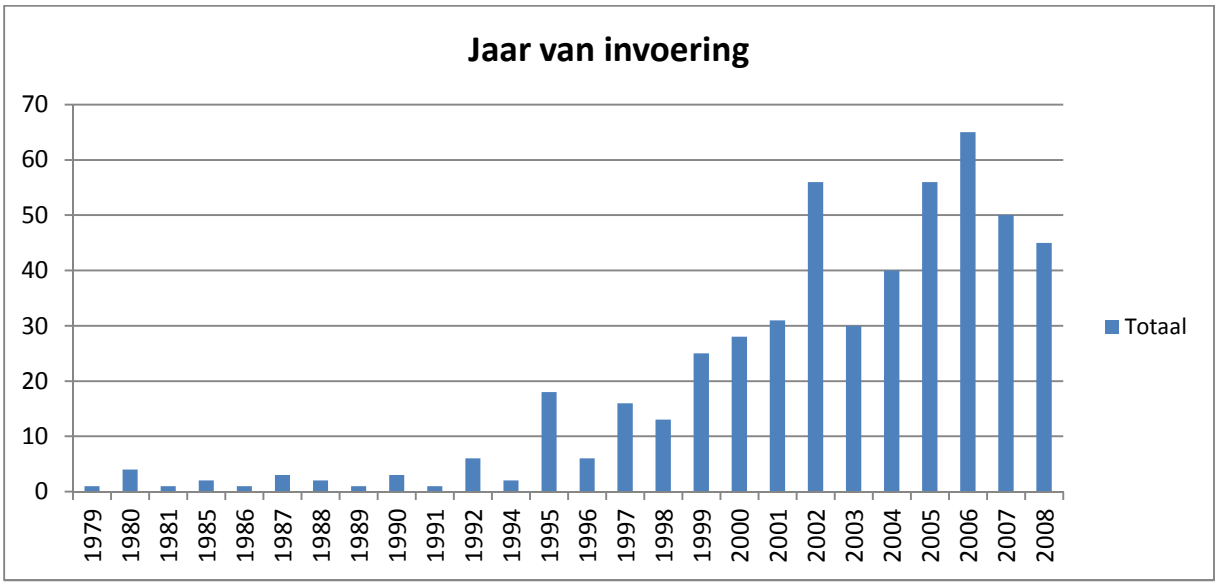
Hieruit kan worden afgeleid dat in 60 % van de gevallen een standaard pakket toereikend is. Tegelijkertijd betekent dit dat in 40 % van de gevallen sprake is van (aanvullend) maatwerk. Vanuit het belang van changemanagement dient daarbij in het bijzonder aandacht dient te worden besteedt aan het totstandkomingsproces van de functionele specificaties, testen en acceptatie van de ontwikkelde aanpassingen.

Ouderdom van de pakketten

De ontwikkeling van pakketten gaat snel. Niet alleen de (technische) mogelijkheden nemen toe maar ook de behoefte aan functionaliteit neemt toe. Het is belangrijk dat de functionaliteit van het pakket aan blijft sluiten bij de behoefte van de organisatie. Als deze aansluiting niet (meer) bestaat, is de kans op het ontstaan van subsystemen groot. Mogelijke gevolgen zijn:

- Niet geformaliseerde (sub) administraties;
- Niet meer actueel zijn van het oorspronkelijke systeem;
- Inefficiëntie.

Om inzicht te krijgen in de levensduur van een pakket wordt in het assessment gevraagd naar het jaar van invoering van de pakketten. De navolgende grafiek toont de resultaten.



Grafiek: Ouderdom pakketten

Omdat de assessments over meerdere jaren zijn uitgevoerd en een vertekend beeld te voorkomen zijn de gegevens over de pakketten die in 2009 en 2012 zijn ingevoerd buiten beschouwing gelaten.

Uit de grafiek kan onder andere worden afgeleid dat een groot deel van de pakketten meer dan 5 jaar geleden is ingevoerd. Het lijkt erop dat dat de economische levensduur niet altijd maatgevend is voor de (langere technische) gebruiksduur van een pakket. Uiteraard speelt daarbij ook de dynamiek in een branche een rol. Immers als er niets veranderd kan de sofware nog prima blijven voldoen. En hoe langer software kan worden gebruikt des te groter is het rendement. Evenwel kan ook ongewild een spanningsveld ontstaan als concurrenten wel investeren in (vernieuwende) sofware en ligt er een aandachtspunt om met de cliënt te bespreken.