Toelichting
IT Audit Essentials™

Dit document geeft een toelichting op het online self assessment IT Audit Essentials™.

Wij adviseren u dit document door te nemen voordat u met het invullen begint. Hierdoor krijgt u inzicht in de vragen, kunt u de antwoorden voorbereiden, eventueel afstemmen met collega's en het online invullen vergemakkelijken.

De uitkomsten van het self assessment worden door uw accountant met u besproken.

Inhoudsopgave

1. Inleiding

Doel IT Audit Essentials self-assessment

In het kader van de controle is het noodzakelijk dat de accountant een beeld heeft van de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking.
De automatiseringsomgeving en de daarin getroffen beheermaatregelen kunnen van invloed zijn op de aanpak en uitvoering van de controlewerkzaamheden.

Het doel van het **self-assessment** is het op een gestructureerde wijze verzamelen van informatie die in dit verband nodig is.

De uitkomsten dragen bij aan een doelmatige, doeltreffende uitvoering van de werkzaamheden van de accountant en maakt het mogelijk de dienstverlening beter op uw specifieke situatie af te stemmen.

Inhoud assessment

Het assessment bestaat uit de volgende onderdelen:

Algemene gegevens
Hierbij wordt gevraagd enkele algemene gegevens in te vullen over uw bedrijf en de contactpersoon.

Let op: Vergeet niet de naam van uw **accountantskantoor** en het **referentienummer** in te vullen. Zonder deze gegevens kunnen de uitkomsten niet worden verwerkt.

Typering automatiseringsomgeving
Bij dit onderdeel wordt een aantal vragen gesteld over uw automatiseringsomgeving. Doel van deze vragen is te komen tot een typering van uw automatiseringsomgeving.
In verband met de

AVG
Tevens zijn een aantal vragen opgenomen ivm de invoering van de Algemene verordening gegevensbescherming (AVG).

Cybersecurity Health Check
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 is nog steeds een belangrijk wapen in de strijd. Om deze reden is de Cyber Security Check opgenomen.

IT Landschap
Dit deel is gericht op het verkrijgen van informatie over de functiegebieden waarin automatisering worden toegepast en de typen en aard van systemen die daarbij worden toegepast.

Werkwijze en procedures
Dit deel is gericht op het verkrijgen van informatie over werkwijzen en procedures die worden toegepast.

Aan het eind van elk onderdeel is er de gelegenheid om daar waar nodig aanvullende informatie en/of toelichting te geven.

Invullen assessment

Voordat u de antwoorden online gaat invullen, raden wij u aan de beantwoording van de vragen aan de hand van dit document voor te bereiden.

Na de voorbereiding kunt u op elk willekeurig moment starten met het online invullen door opnieuw in te loggen via de link in de uitnodiging. Zolang het invullen niet volledig is afgerond, kunt u het invullen tussentijds beëindigen en op een later moment vervolgen. Volg daarvoor de aanwijzingen voor het aanmaken van een link naar de reeds gegeven antwoorden. Zonder deze link kunt u de antwoorden niet meer benaderen Ook kunt u dan desgewenst uw antwoorden nog wijzigen.

Het invullen van het assessment is eenvoudig en behoeft geen uitgebreide uitleg. Daarom wordt volstaan met de belangrijkste punten.

Vanwege het gebruiksgemak hebben veel vragen een niet verplicht karakter. Om de toegevoegde waarde van de uitkomsten van het assessment voor uw organisatie zo groot mogelijk te maken, is het van belang om alle vragen zo goed en zo volledig mogelijk te beantwoorden.

Advies: Laat alleen een antwoord open als u het echt niet weet.

Navigatie
Door middel van onderstaande knoppen kunt u door de schermen van het assessment navigeren:

Met de knop *Vorige* gaat u naar de voorgaande pagina
Met de knop *Volgende* gaat u naar de volgende pagina

Let op: Tijdens het invullen worden de antwoorden niet automatisch opgeslagen. Dit gebeurt pas als u daarvoor zelf kiest. Als u ervoor kiest om de vragenlijst in een keer in te vullen adviseren wij om ook tussentijds de resultaten op te slaan. Zie onderstaand.

Opslaan en later doorgaan
U kunt tussentijds het invullen onderbreken door rechtsboven in uw browser te klikken op .
Om de ingevulde antwoorden te bewaren **dient u voor het verlaten** van een scherm de link naar de vragenlijst op te slaan. Zie onderstaand scherm.

U kunt de link aanwijzen en met een rechtermuisklik de link opslaan op een door u gewenste locatie. U kunt de link echter ook mailen naar het door u op te geven email adres.

Als u later via de link terugkeert, komt u terug op het punt waarop het assessment is verlaten.

Aanleveren digitale informatie

Aan het einde van het assessment wordt gevraagd om digitaal aanvullende informatie mee te sturen. Het aanleveren van deze informatie is van belang om uw antwoorden in een zo goed mogelijke context te kunnen plaatsen.

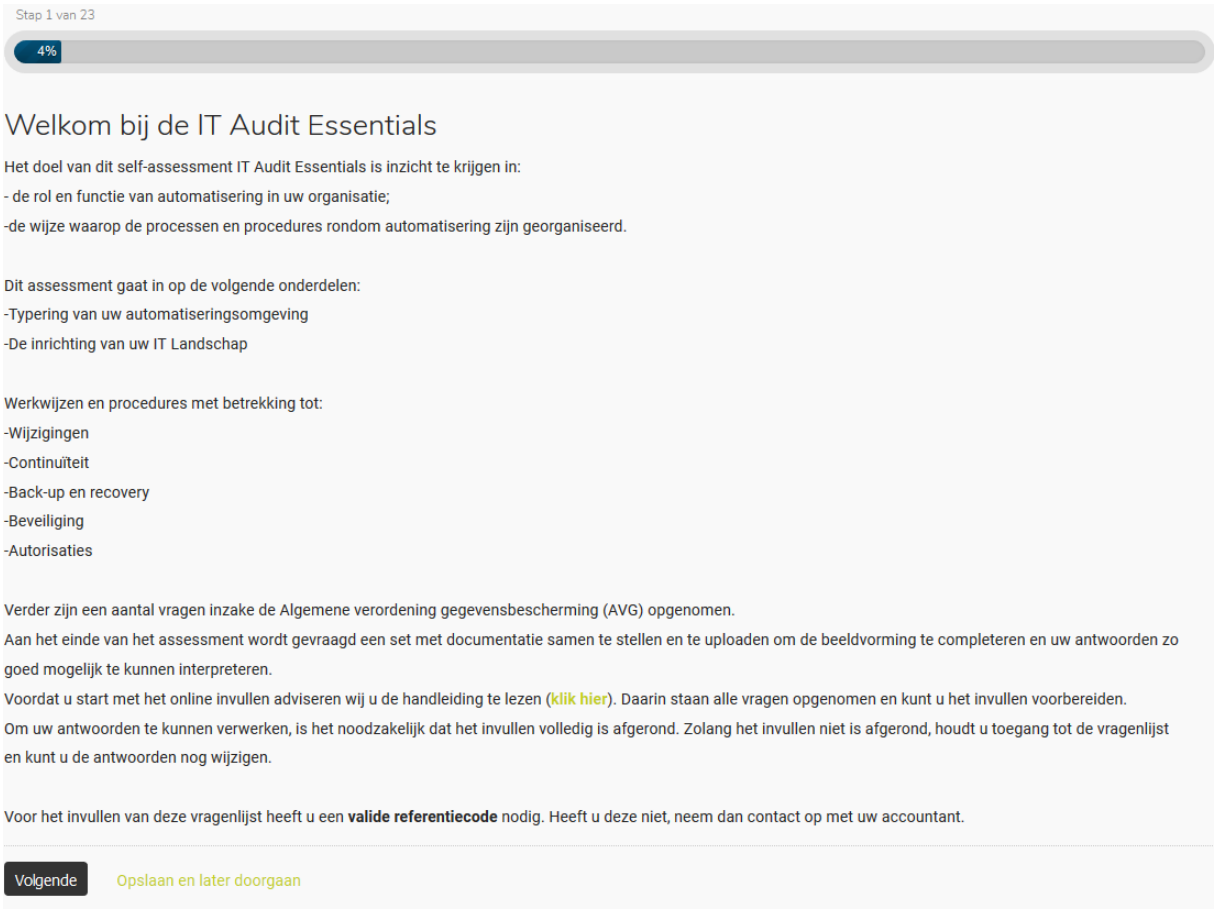
Versturen assessment
Als u zeker bent van de antwoorden, de aanvullende informatie hebt geselecteerd en eventueel een toelichting hebt gegeven kunt u het assessment versturen door op de knop versturen te klikken.

Daarmee wordt het assessment definitief gemaakt, verzonden naar onze database en kunnen de antwoorden niet meer worden gewijzigd. Daarna heeft u dan ook geen toegang meer tot de vragenlijst.

Per email ontvangt u dan een opgave van de gegeven antwoorden voor uw eigen administratie.

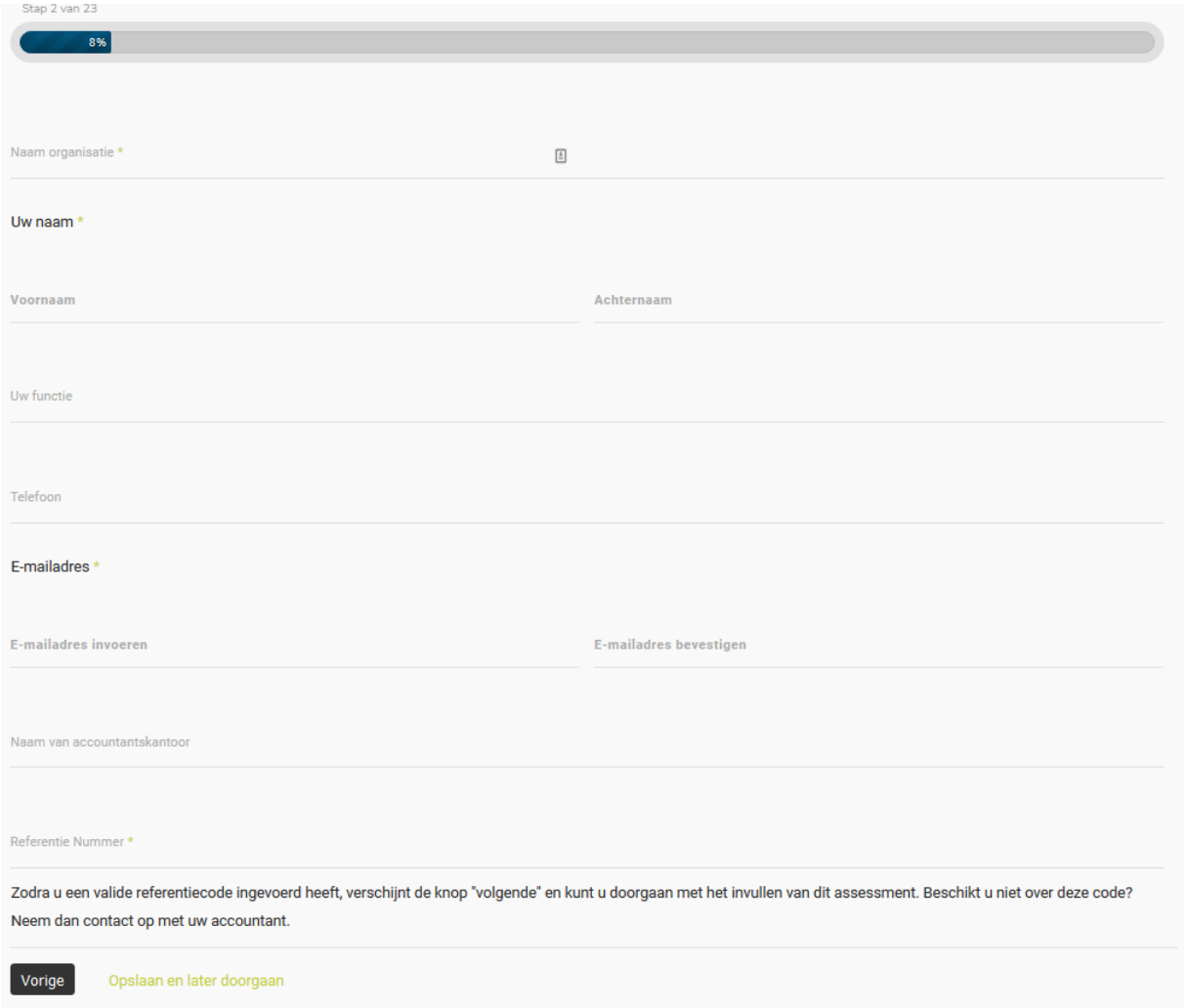
<u>Vragen en antwoorden</u>
De pagina’s hierna geven een overzicht van de vragen en de antwoorden die worden verwacht.
Aan de hand hiervan kunt u zich een beeld vormen van de inhoud en het invullen van uw antwoorden voorbereiden.

2. Welkomstscherm

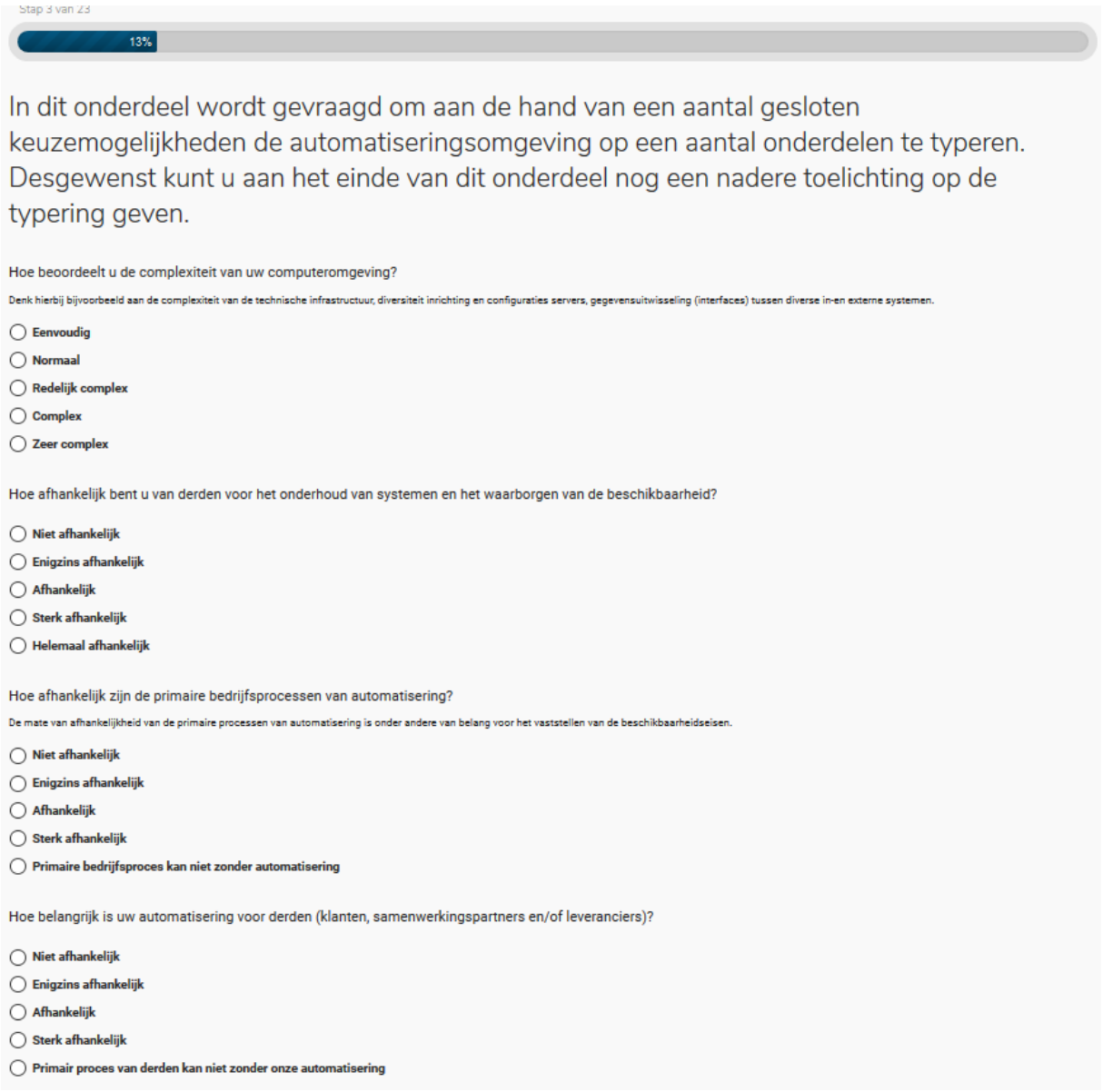


3. Algemene gegevens

Dit scherm is verplicht in te vullen. Vergeet hierbij niet de **naam van uw accountantskantoor en het opgegeven referentienummer** in te vullen. Als de validatie van het referentienummer niet slaagt kunt u het assessment niet invullen.



4. Typering van uw automatiseringsomgeving


Stap 3 van 23

13%

In dit onderdeel wordt gevraagd om aan de hand van een aantal gesloten keuzemogelijkheden de automatiseringsomgeving op een aantal onderdelen te typeren. Desgewenst kunt u aan het einde van dit onderdeel nog een nadere toelichting op de typering geven.

Hoe beoordeelt u de complexiteit van uw computeromgeving?

Denk hierbij bijvoorbeeld aan de complexiteit van de technische infrastructuur, diversiteit inrichting en configuraties servers, gegevensuitwisseling (interfaces) tussen diverse in-en externe systemen.

- ◯ Eenvoudig
- ◯ Normaal
- ◯ Redelijk complex
- ◯ Complex
- ◯ Zeer complex

Hoe afhankelijk bent u van derden voor het onderhoud van systemen en het waarborgen van de beschikbaarheid?

- ◯ Niet afhankelijk
- ◯ Enigzins afhankelijk
- ◯ Afhankelijk
- ◯ Sterk afhankelijk
- ◯ Helemaal afhankelijk

Hoe afhankelijk zijn de primaire bedrijfsprocessen van automatisering?

De mate van afhankelijkheid van de primaire processen van automatisering is onder andere van belang voor het vaststellen van de beschikbaarheidseisen.

- ◯ Niet afhankelijk
- ◯ Enigzins afhankelijk
- ◯ Afhankelijk
- ◯ Sterk afhankelijk
- ◯ Primaire bedrijfsproces kan niet zonder automatisering

Hoe belangrijk is uw automatisering voor derden (klanten, samenwerkingspartners en/of leveranciers)?

- ◯ Niet afhankelijk
- ◯ Enigzins afhankelijk
- ◯ Afhankelijk
- ◯ Sterk afhankelijk
- ◯ Primair proces van derden kan niet zonder onze automatisering

Hoe afhankelijk is de financiële informatievoorziening van de betrouwbare werking van uw automatiseringsomgeving?

- ◯ **Niet afhankelijk**
- ◯ **Enigzins afhankelijk**
- ◯ **Afhankelijk**
- ◯ **Sterk afhankelijk**
- ◯ **Helemaal afhankelijk**

Op welke wijze komt de periodieke financiële informatievoorziening tot stand?

- ◯ **Rechtstreeks uit primaire voorzieningen**
- ◯ **Via een specifieke rapportage tool**
- ◯ **Via overname en bewerkingen van gegevens (bijvoorbeeld in MS Excel)**

Hoe vaak worden wijzigingen doorgevoerd in de automatiseringsomgeving?

De frequentie van het doorvoeren van wijzigingen kan iets zeggen over de stabiliteit van systemen en geeft het belang van een goed wijzigingenbeheer aan.

- ◯ **Bijna geen wijzigingen**
- ◯ **Weinig wijzigingen**
- ◯ **Regelmatig wijzigingen**
- ◯ **Veel wijzigingen**
- ◯ **Voortdurend wijzigingen**

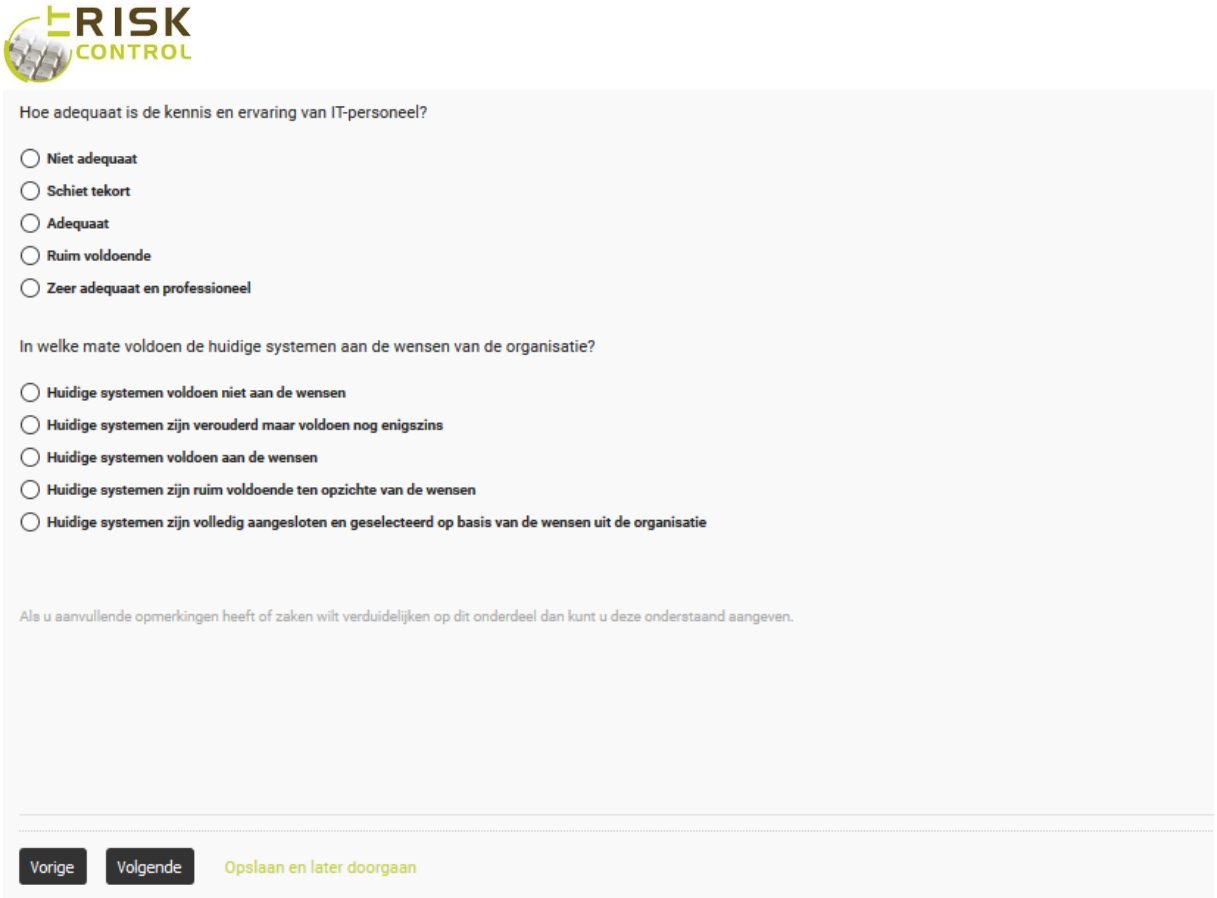
Hoe stabiel zijn uw huidige systemen?

- ◯ **Zeer stabiel, vrijwel nooit storingen**
- ◯ **Stabiel, weinig tot geen storingen**
- ◯ **Stabiel**
- ◯ **Enigszins stabiel**
- ◯ **Niet stabiel**

In welke mate is het management bewust van het strategisch belang van IT en de bijbehorende risico's?

Het bewustzijn van het management kan zich op vele manieren uiten. Bijvoorbeeld door frequent overleg, actieve betrokkenheid bij beslissingen, pro-activiteit, etc.

- ◯ **Management kijkt niet naar automatisering om**
- ◯ **Management is zich enigszins bewust van belang en risicos**
- ◯ **Management is zich bewust van belang en risicos**
- ◯ **Management is zich bewust van belang en risicos en handelt daar ook naar**
- ◯ **Management is actief betrokken bij IT vanwege een sterk bewustzijn van het belang en mogelijke risicos**


Hoe adequaat is de kennis en ervaring van IT-personeel?
Niet adequaat
Schiet tekort
Adequaat
Ruim voldoende
Zeer adequaat en professioneel
In welke mate voldoen de huidige systemen aan de wensen van de organisatie?
Huidige systemen voldoen niet aan de wensen
Huidige systemen zijn verouderd maar voldoen nog enigszins
Huidige systemen voldoen aan de wensen
Huidige systemen zijn ruim voldoende ten opzichte van de wensen
Huidige systemen zijn volledig aangesloten en geselecteerd op basis van de wensen uit de organisatie
Als u aanvullende opmerkingen heeft of zaken wilt verduidelijken op dit onderdeel dan kunt u deze onderstaand aangeven.
Vorige
Volgende
Opslaan en later doorgaan

5. Algemene verordening gegevensbescherming (AVG)

Stap 4 van 21

19%

AVG

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. Voor meer informatie. 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).

Verwerkt u persoonsgegevens?

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.

Toelichting persoonsgegevens

- ◯ **Ja**
- ◯ **Nee**

Kent u de rechten van betrokkenen?

Onder de AVG krijgen de mensen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten. Zorg er daarom voor dat zij hun privacyrechten goed kunnen uitoefenen. Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen. Ook kunnen mensen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

Toelichting rechten van betrokkenen

- ◯ **Ja**
- ◯ **Nee**

Heeft u de gegevensverwerking in kaart?

Documenteert u welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt? Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt. Het bijhouden van een register van verwerkingsactiviteiten is onderdeel van de verantwoordingsplicht. U kunt het register ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

Toelichting gegevensverwerking in kaart

- ◯ **Ja**
- ◯ **Nee**

Heeft u een procedure voor het registreren en melden van datalekken?

De AVG stelt strenge eisen aan de eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

Toelichting registreren en melden datalekken

- ◯ **Ja**
- ◯ **Nee**

Heeft u uw gegevensverwerking uitbesteed aan een verwerker?

Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw verwerkers nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Toelichting uitbesteding gegevensverwerking

- ◯ **Ja**
- ◯ **Nee**


Heeft u toestemming van betrokkenen?
Voor sommige gegevensverwerkingen hebt u toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.
Toelichting toestemming betrokkenen
Ja
Nee
Vorige
Volgende
Opslaan en later doorgaan

6. Cybersecurity Health Check

Stap 5 van 24

20%

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 Meer informatie.

Wilt u de vragen over cybersecurity invullen?

- ○ **Ja**
- ○ **Nee**

Vorige | Volgende | Opslaan en later doorgaan

Instructies

Hierna volgen de vragen van de check. De check is geen uitputtende lijst, maar bedoeld als een goede start om de belangrijkste cyberrisco's in beeld te brengen en te mitigeren.

Geef bij iedere vraag aan of dit voldoende is geïmplementeerd binnen uw organisatie en ga daarbij uit van de huidige stand.

Identificatie

Is de verantwoordelijkheid voor cybersecurity binnen de directie belegd en wordt cybersecurity periodiek binnen de directie besproken?

- ○ **Ja**
- ○ **Nee**

Toelichting verantwoordelijkheid voor cybersecurity

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?

- ○ **Ja**
- ○ **Nee**

Toelichting belangrijkste kroonjuwelen

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?

- ○ **Ja**
- ○ **Nee**

Toelichting in kaart brengen belangrijkste cyberrisico's en -dreigingen

Bescherming

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)?

- ◯ Ja
- ◯ Nee

Toelichting bijscholing

Is bij zowel u als een eventuele derde partij het patch management (bijwerken, testen en installeren van software) op orde?

- ◯ Ja
- ◯ Nee

Toelichting patch management

Is bij zowel u als een eventuele derde partij het toegangsbeheer (incl. intrekken toegang van gebruikers na functiewisseling of - beëindiging) op orde?

- ◯ Ja
- ◯ Nee

Toelichting toegangsbeheer

Is bij zowel u als een eventuele derde partij het maken van back-ups op orde?

- ◯ Ja
- ◯ Nee

Toelichting het maken van back-ups

Worden deze periodiek uitgevoerd en wordt de effectiviteit ervan regelmatig getest? Zo nee, wat doet u wel aan eventuele periodieke controles?

- ◯ Ja
- ◯ Nee

Toelichting uitvoering periodiek testen

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?

- ◯ Ja
- ◯ Nee

Toelichting effectieve maatregelen

Detectie

Maakt uw organisatie gebruik van logging (log files), al dan niet centraal geaggregeerd? Wordt deze ook actief geanalyseerd, zodat monitoring van incidenten plaatsvindt?

- ◯ Ja
- ◯ Nee

Toelichting gebruik van logging

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
- ◯ Nee

Toelichting dreiging van ransomware

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
- ◯ Nee

Toelichting dreiging van virussen en trojans

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?

- ◯ Ja
- ◯ Nee

Toelichting dreiging van diefstal van informatie

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?

Toelichting dreiging van ongeautoriseerde toegang tot servers

- ◯ Ja
- ◯ Nee

Toetst uw organisatie de effectiviteit van de getroffen beveiligingsmaatregelen door het uitvoeren van een kwetsbaarhedenscan?

Het automatisch scannen van aan internet gekoppelde systemen en applicaties op de aanwezigheid van publiekelijk bekende kwetsbaarheden en configuratiefouten.

Toelichting uitvoeren kwetsbaarhedenscan

- ◯ Ja
- ◯ Nee

Toetst uw organisatie de effectiviteit van de getroffen beveiligingsmaatregelen door het uitvoeren van penetratietesten?

Beveiligingstesten van aan internet gekoppelde systemen en applicaties en/of de kantoorautomatisering.

Toelichting uitvoeren penetratietesten

- ◯ Ja
- ◯ Nee

Toetst uw organisatie de effectiviteit van de getroffen beveiligingsmaatregelen door het uitvoeren van red-teaming?

Op basis van scenario's tracht een hacker ongeautoriseerde toegang te verkrijgen tot uw informatie.

Toelichting uitvoeren red-teaming

- ◯ Ja
- ◯ Nee

Reactie

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?

Toelichting communicatieplan

- ◯ Ja
- ◯ 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?

Toelichting crisisplan

- ◯ Ja
- ◯ 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?

Toelichting periodieke oefening

- ◯ Ja
- ◯ Nee

Herstel

Heeft uw organisatie een herstelplan opgesteld, dat u in staat stelt op tijd de bedrijfsvoering te hervatten (voordat de schade te groot is)?

- ◯ Ja
- ◯ Nee

Toelichting herstelplan

Zijn uw back-upvoorzieningen zodanig ingericht dat u snel en efficiënt getroffen systemen kunt herstellen naar normale operatie en test u dit regelmatig?

- ◯ Ja
- ◯ Nee

Toelichting back-upvoorzieningen

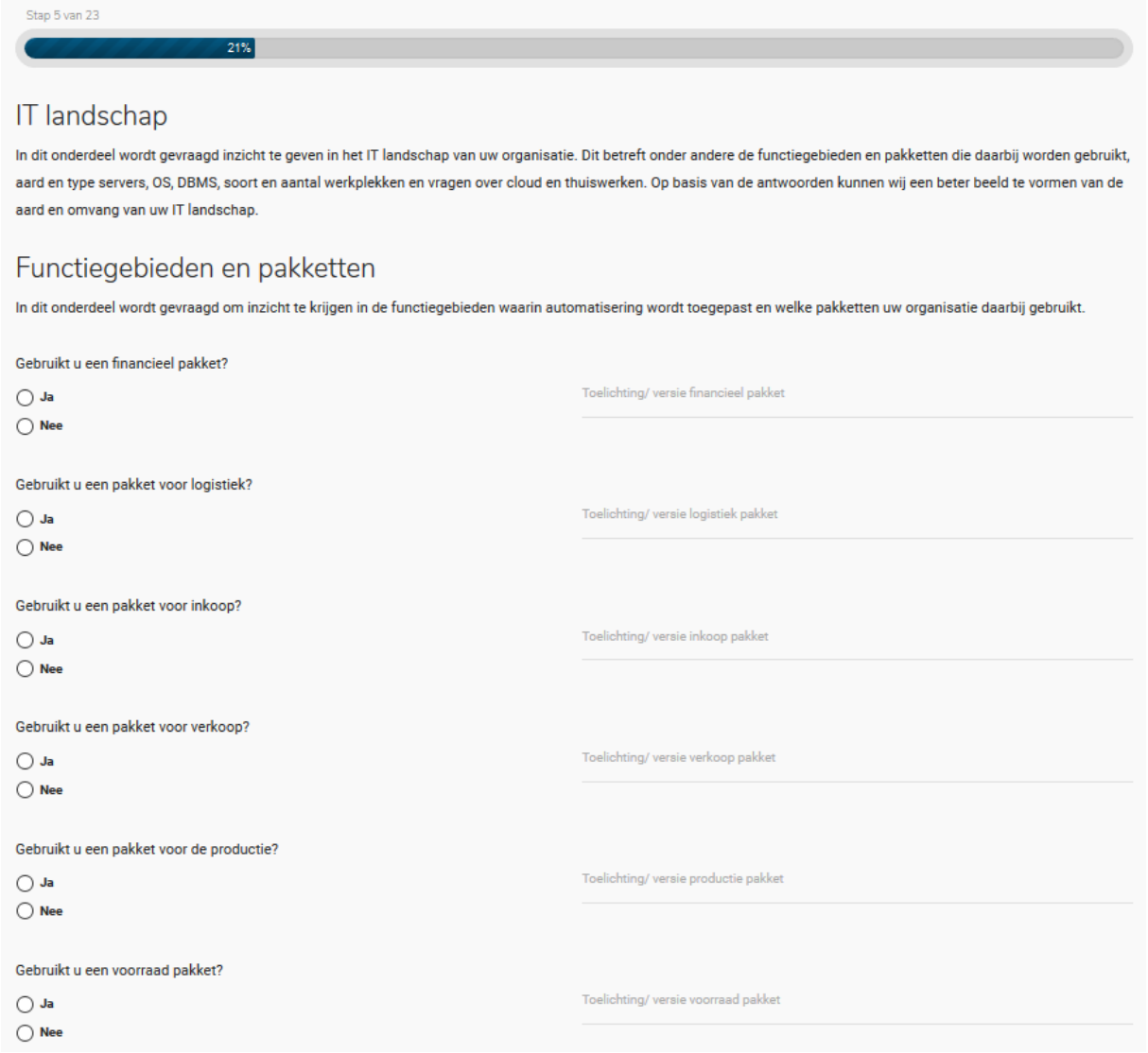
Heeft uw organisatie processen en middelen om te leren van opgetreden cyberincidenten om deze in de toekomst te voorkomen, sneller te detecteren of beter op te reageren?

- ◯ Ja
- ◯ Nee

Toelichting cyberincidenten voorkomen

Vorige | Volgende | Opslaan en later doorgaan

7. IT landschap



Gebruikt u een service pakket?

- ◯ Ja
- ◯ Nee

Toelichting/ versie service pakket

Gebruikt u een pakket voor personeelszaken?

- ◯ Ja
- ◯ Nee

Toelichting/ versie personeelszaken pakket

Gebruikt u een salaris pakket?

- ◯ Ja
- ◯ Nee

Toelichting/ versie salaris pakket

Gebruikt u een CRM pakket?

- ◯ Ja
- ◯ Nee

Toelichting/ versie CRM pakket

Gebruikt u een CMS pakket?

- ◯ Ja
- ◯ Nee

Toelichting/ versie CMS pakket

Gebruikt u een pakket voor kantoorautomatisering?

- ◯ Ja
- ◯ Nee

Toelichting/ versie pakket kantoorautomatisering

Gebruikt u een pakket voor web verkoop?

- ◯ Ja
- ◯ Nee

Toelichting/ versie web verkoop pakket

Gebruikt u een managementinformatie/BI pakket?

- ◯ Ja
- ◯ Nee

Toelichting/ versie managementinformatie/BI pakket

Gebruikt u nog andere automatiseringspakketten?

- ◯ Ja
- ◯ Nee

Toelichting/ versie andere automatiseringspakketten

Vorige | Volgende | Opslaan en later doorgaan

Bij de volgende vragen gaat het om de meer technische kant van het IT Landschap en de beveiliging tegen bedreigingen.

Doordat het open vragen zijn is het wel van belang om uw situatie zo concreet mogelijk te beschrijven. Beschikt u al over beschrijvingen of andere documentatie waaruit het antwoord op de vraag blijkt. Dan kunt u volstaan met een korte opmerking en verwijzen naar de betreffende documenten. Deze moet u dan uiteraard wel, aan het einde van dit assessment, als bijlage toevoegen.

Om u bij de beantwoording van de vragen te kunnen voorzien van voorbeelden en u te ondersteunen zijn verwijzingen naar Wikipedia opgenomen.

Servers en Operatingsystemen

Kunt u aangeven van welke type servers u gebruik maakt en welke Operating Systemen en versies deze servers gebruiken?

Nadere toelichting en voorbeelden voor type servers
Nadere toelichting en voorbeelden voor Operatingsystemen

Geef hier een zo concreet mogelijke beschrijving van uw situatie en/of neem een verwijzing op naar documenten die u met het assessment instuurt.

Databasemanagement systemen

Kunt u aangeven welke Databasemanagement Systemen worden gebruikt en waarvoor deze worden gebruikt?

Nadere toelichting en voorbeelden over databasemanagementsystemen

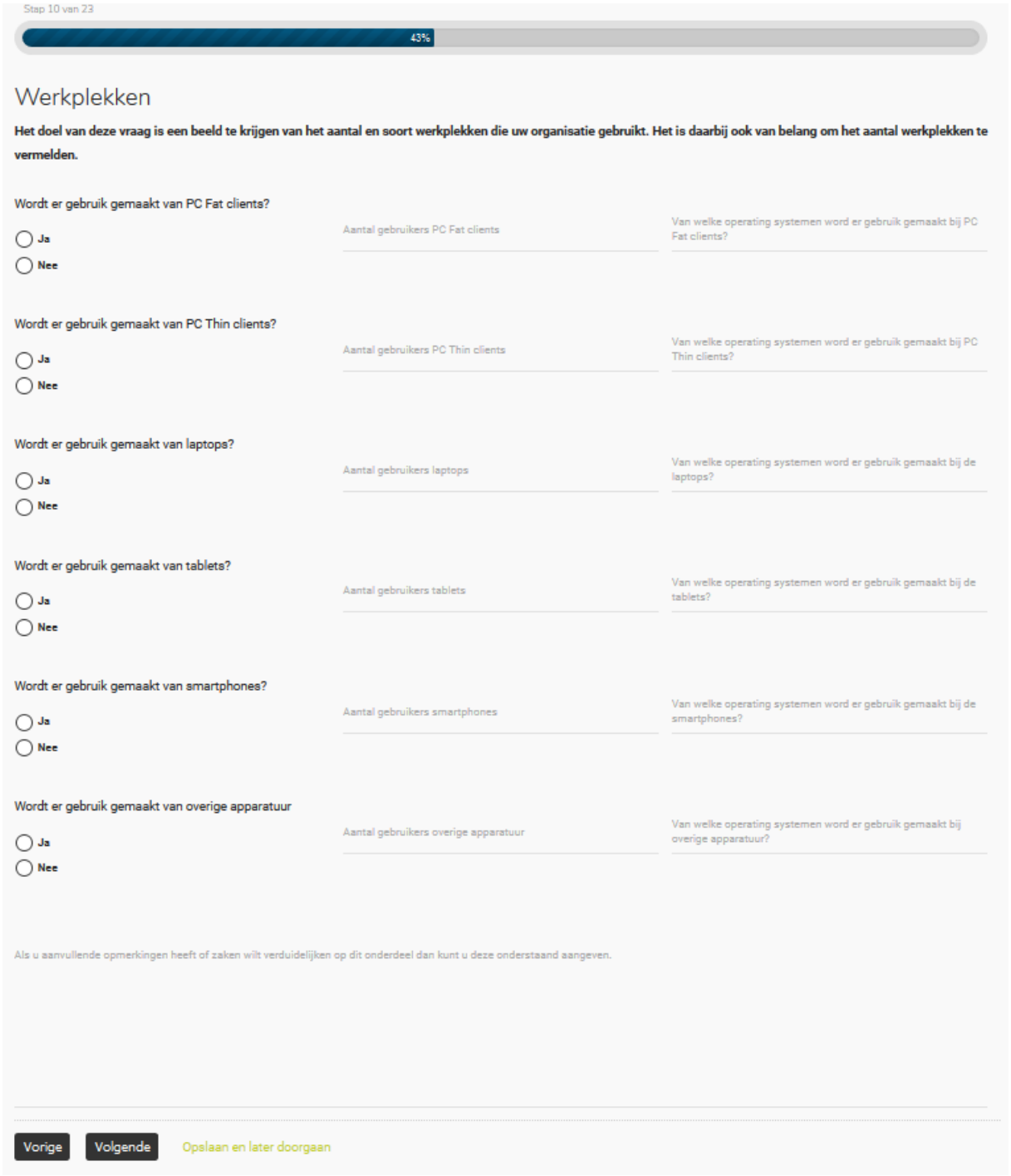
Geef hier een zo concreet mogelijke beschrijving van uw situatie en/of neem een verwijzing op naar documenten die u met het assessment instuurt.

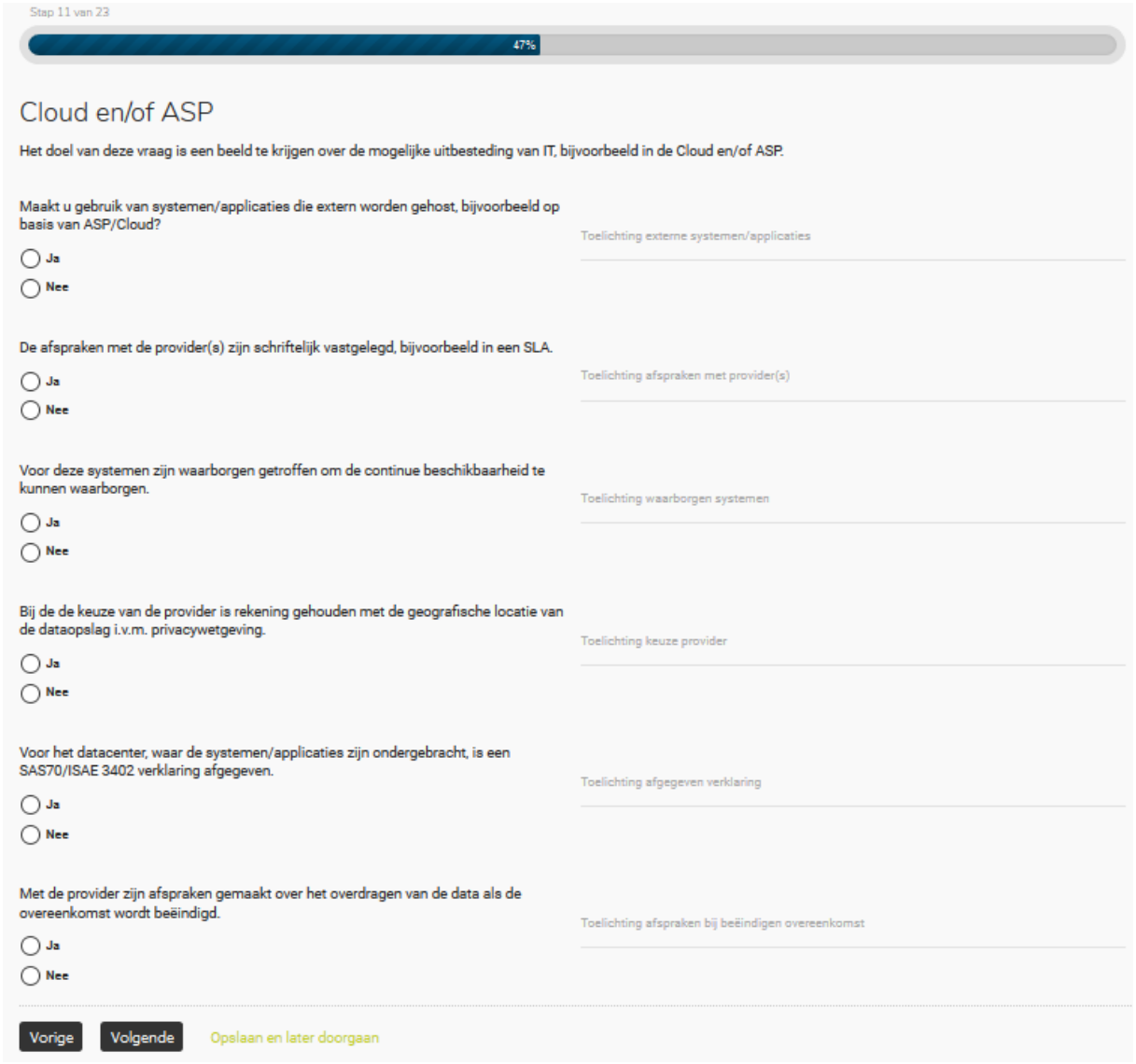
Bescherming tegen virussen, inbraken en DDOS e.d.

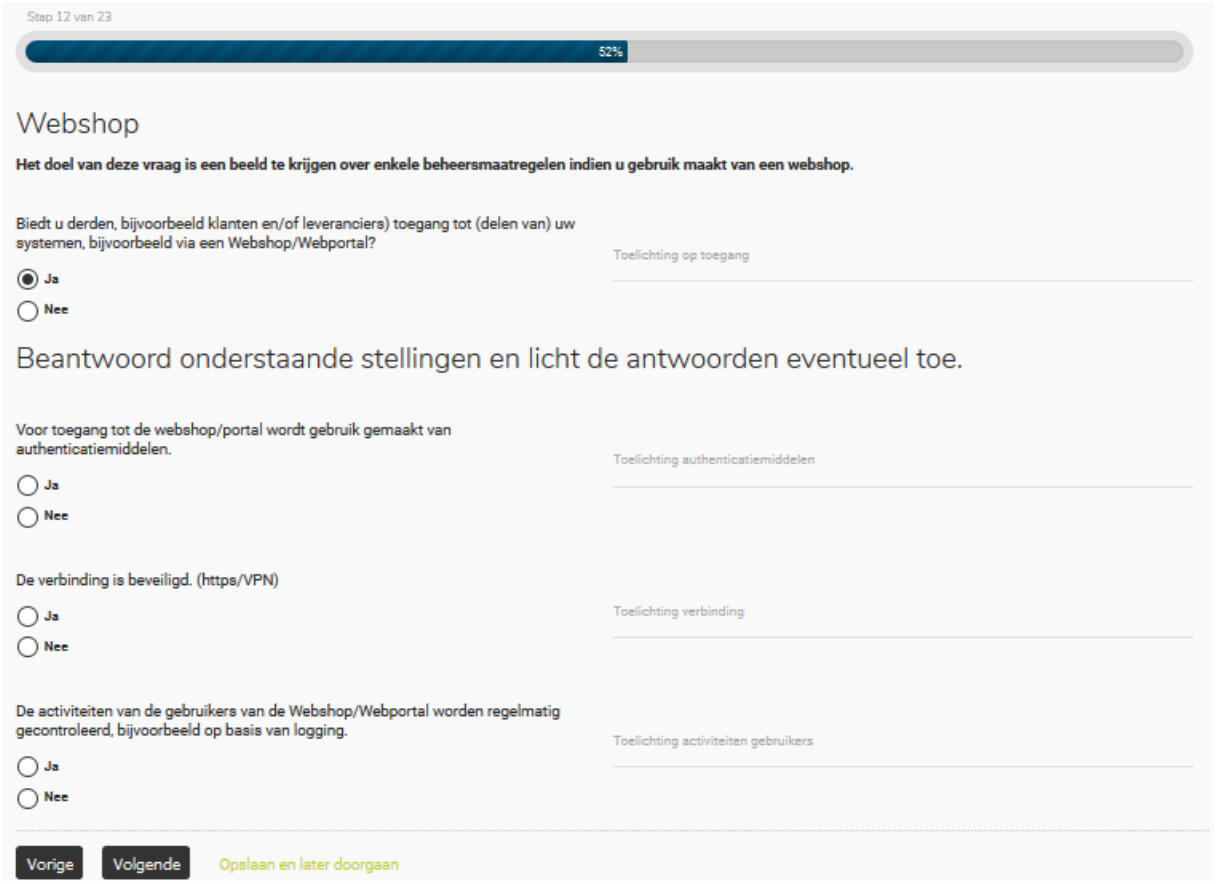
Kunt u aangeven welke maatregelen zijn getroffen voor het beveiligen van uw informatievoorziening? Dit kunnen zowel maatregelen in de software, hardware zijn als fysieke en/of procedurele maartregelen zijn.

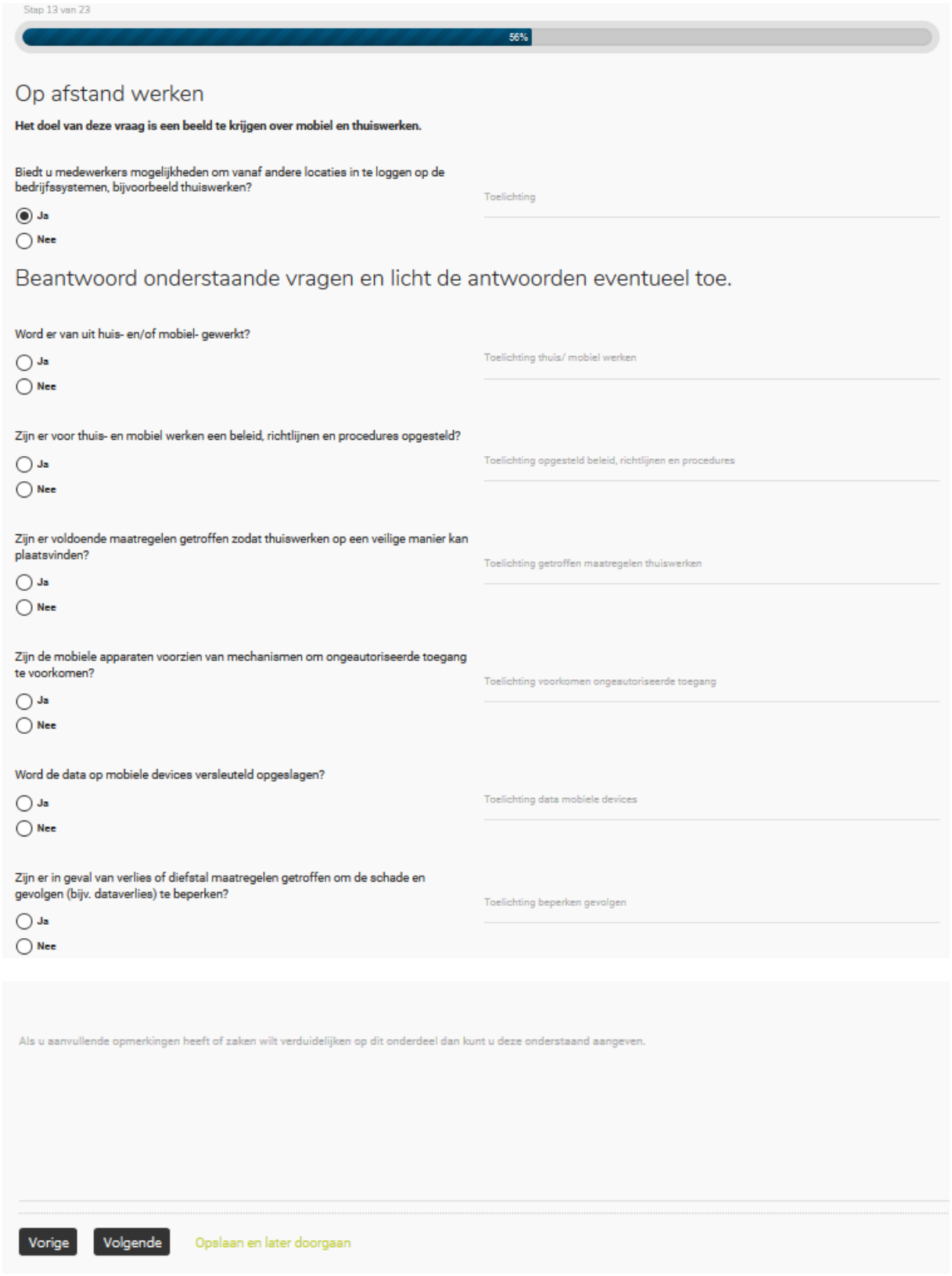
Nadere toelichting en voorbeelden over informatiebeveiliging

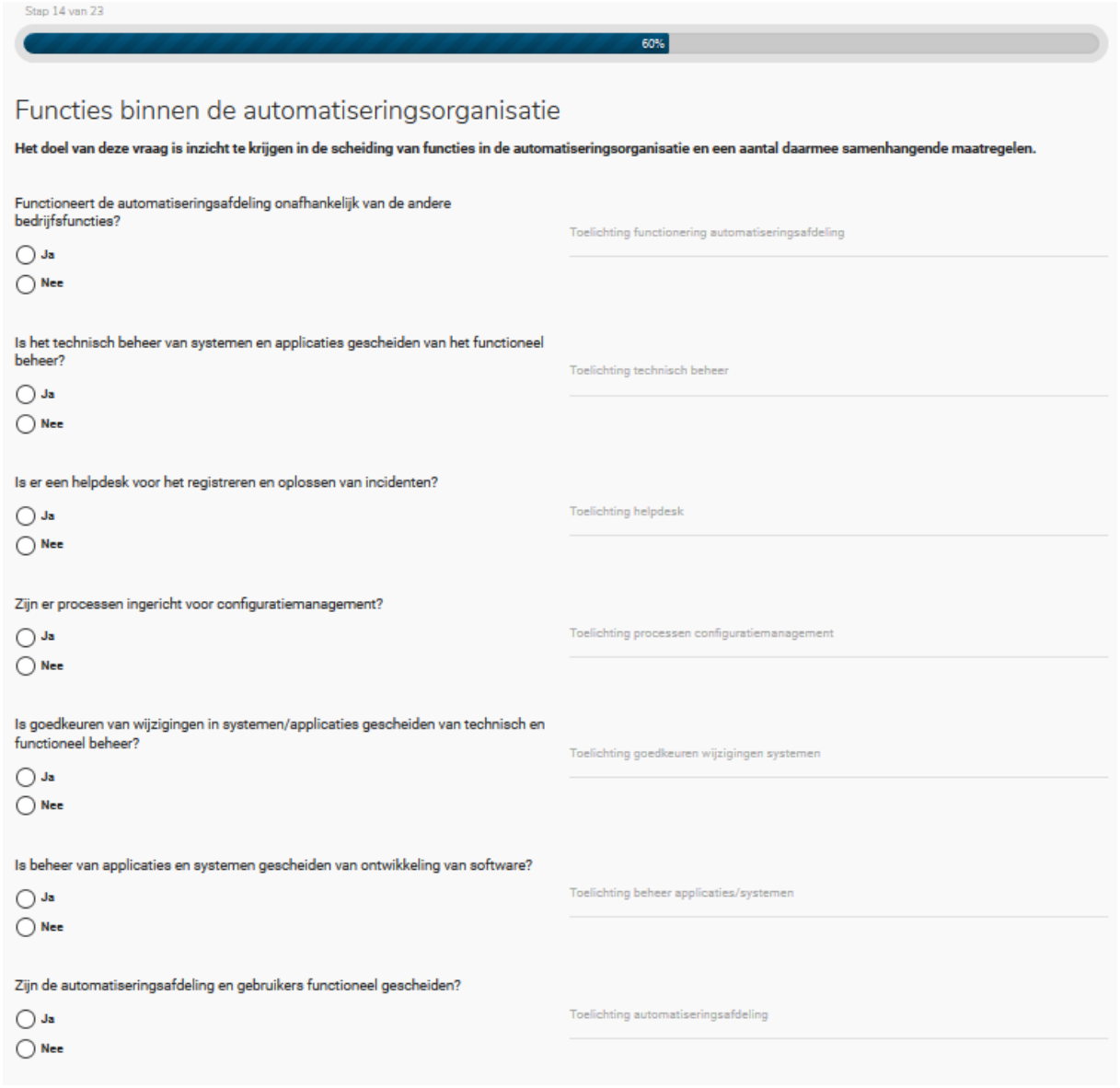
Geef hier een zo concreet mogelijke beschrijving van uw situatie en/of neem een verwijzing op naar documenten die u met het assessment instuurt.

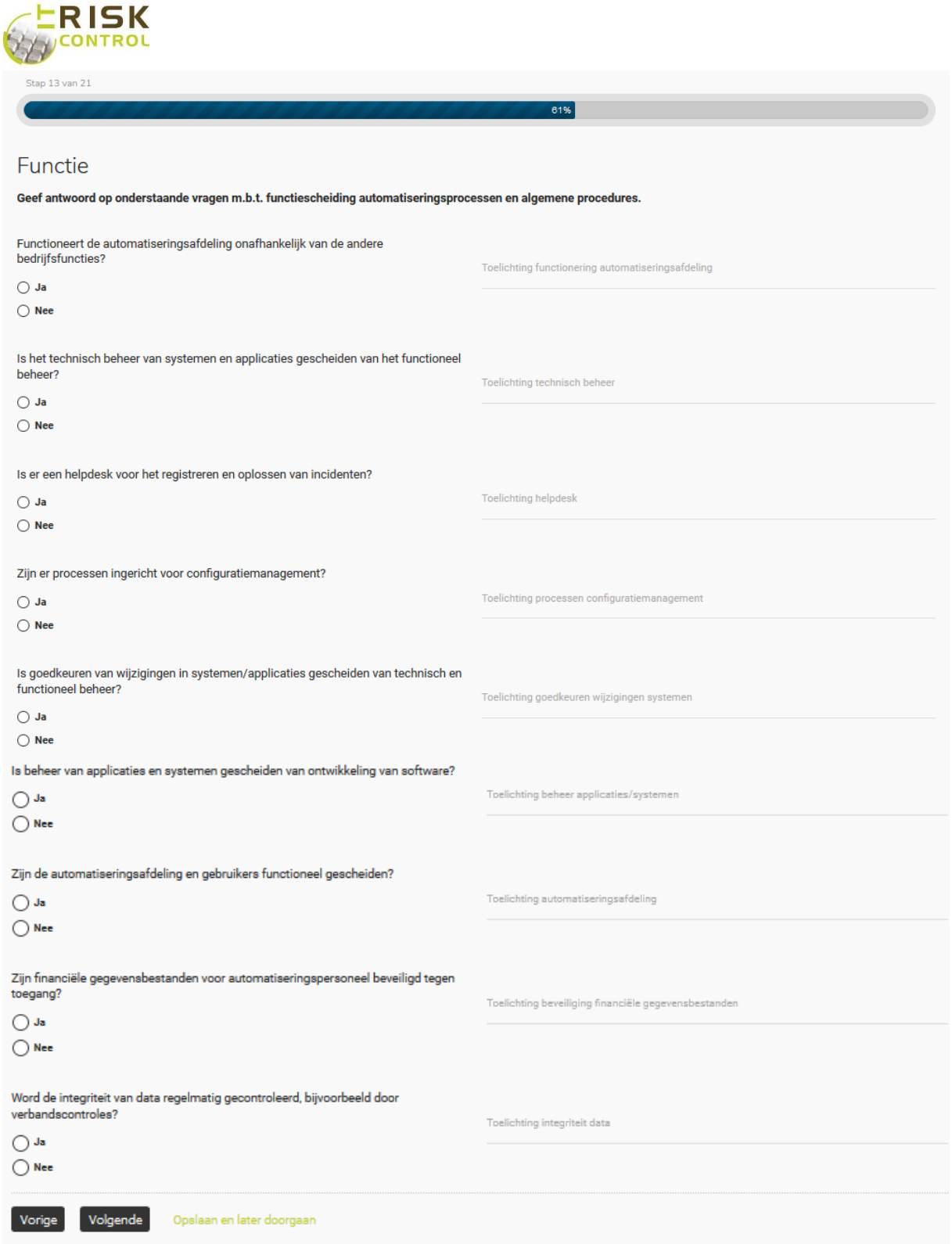

Stap 10 van 23
43%
Werkplekken
Het doel van deze vraag is een beeld te krijgen van het aantal en soort werkplekken die uw organisatie gebruikt. Het is daarbij ook van belang om het aantal werkplekken te vermelden.
Wordt er gebruik gemaakt van PC Fat clients?
Ja
Nee
Aantal gebruikers PC Fat clients
Van welke operating systemen word er gebruik gemaakt bij PC Fat clients?
Wordt er gebruik gemaakt van PC Thin clients?
Ja
Nee
Aantal gebruikers PC Thin clients
Van welke operating systemen word er gebruik gemaakt bij PC Thin clients?
Wordt er gebruik gemaakt van laptops?
Ja
Nee
Aantal gebruikers laptops
Van welke operating systemen word er gebruik gemaakt bij de laptops?
Wordt er gebruik gemaakt van tablets?
Ja
Nee
Aantal gebruikers tablets
Van welke operating systemen word er gebruik gemaakt bij de tablets?
Wordt er gebruik gemaakt van smartphones?
Ja
Nee
Aantal gebruikers smartphones
Van welke operating systemen word er gebruik gemaakt bij de smartphones?
Wordt er gebruik gemaakt van overige apparatuur
Ja
Nee
Aantal gebruikers overige apparatuur
Van welke operating systemen word er gebruik gemaakt bij overige apparatuur?
Als u aanvullende opmerkingen heeft of zaken wilt verduidelijken op dit onderdeel dan kunt u deze onderstaand aangeven.
Vorige
Volgende
Opslaan en later doorgaan

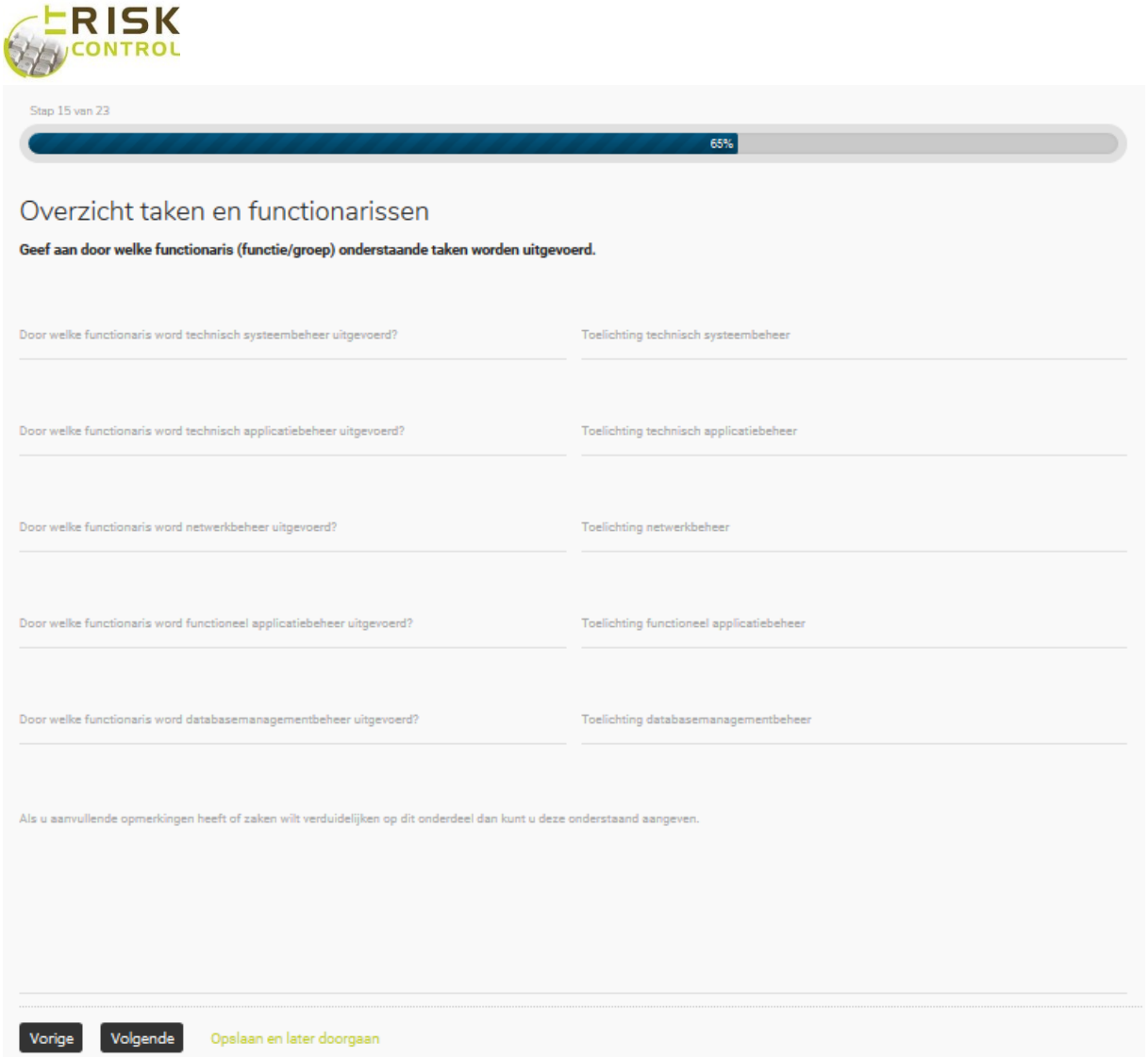

Stap 11 van 23
47%
Cloud en/of ASP
Het doel van deze vraag is een beeld te krijgen over de mogelijke uitbesteding van IT, bijvoorbeeld in de Cloud en/of ASP.
Maakt u gebruik van systemen/applicaties die extern worden gehost, bijvoorbeeld op basis van ASP/Cloud?
Toelichting externe systemen/applicaties
Ja
Nee
De afspraken met de provider(s) zijn schriftelijk vastgelegd, bijvoorbeeld in een SLA.
Toelichting afspraken met provider(s)
Ja
Nee
Voor deze systemen zijn waarborgen getroffen om de continue beschikbaarheid te kunnen waarborgen.
Toelichting waarborgen systemen
Ja
Nee
Bij de de keuze van de provider is rekening gehouden met de geografische locatie van de dataopslag i.v.m. privacywetgeving.
Toelichting keuze provider
Ja
Nee
Voor het datacenter, waar de systemen/applicaties zijn ondergebracht, is een SAS70/ISAE 3402 verklaring afgegeven.
Toelichting afgegeven verklaring
Ja
Nee
Met de provider zijn afspraken gemaakt over het overdragen van de data als de overeenkomst wordt beëindigd.
Toelichting afspraken bij beëindigen overeenkomst
Ja
Nee
Vorige
Volgende
Opslaan en later doorgaan


Stap 12 van 23
52%
Webshop
Het doel van deze vraag is een beeld te krijgen over enkele beheersmaatregelen indien u gebruik maakt van een webshop.
Biedt u derden, bijvoorbeeld klanten en/of leveranciers) toegang tot (delen van) uw systemen, bijvoorbeeld via een Webshop/Webportal?
Toelichting op toegang
Ja
Nee
Beantwoord onderstaande stellingen en licht de antwoorden eventueel toe.
Voor toegang tot de webshop/portal wordt gebruik gemaakt van authenticatiemiddelen.
Toelichting authenticatiemiddelen
Ja
Nee
De verbinding is beveiligd. (https/VPN)
Toelichting verbinding
Ja
Nee
De activiteiten van de gebruikers van de Webshop/Webportal worden regelmatig gecontroleerd, bijvoorbeeld op basis van logging.
Toelichting activiteiten gebruikers
Ja
Nee
Vorige
Volgende
Opslaan en later doorgaan


Stap 13 van 23
56%
Op afstand werken
Het doel van deze vraag is een beeld te krijgen over mobiel en thuiswerken.
Biedt u medewerkers mogelijkheden om vanaf andere locaties in te loggen op de bedrijfssystemen, bijvoorbeeld thuiswerken?
Toelichting
Ja
Nee
Beantwoord onderstaande vragen en licht de antwoorden eventueel toe.
Word er van uit huis- en/of mobiel- gewerkt?
Toelichting thuis/ mobiel werken
Ja
Nee
Zijn er voor thuis- en mobiel werken een beleid, richtlijnen en procedures opgesteld?
Toelichting opgesteld beleid, richtlijnen en procedures
Ja
Nee
Zijn er voldoende maatregelen getroffen zodat thuiswerken op een veilige manier kan plaatsvinden?
Toelichting getroffen maatregelen thuiswerken
Ja
Nee
Zijn de mobiele apparaten voorzien van mechanismen om ongeautoriseerde toegang te voorkomen?
Toelichting voorkomen ongeautoriseerde toegang
Ja
Nee
Word de data op mobiele devices versleuteld opgeslagen?
Toelichting data mobiele devices
Ja
Nee
Zijn er in geval van verlies of diefstal maatregelen getroffen om de schade en gevolgen (bijv. dataverlies) te beperken?
Toelichting beperken gevolgen
Ja
Nee
Als u aanvullende opmerkingen heeft of zaken wilt verduidelijken op dit onderdeel dan kunt u deze onderstaand aangeven.
Vorige
Volgende
Opslaan en later doorgaan

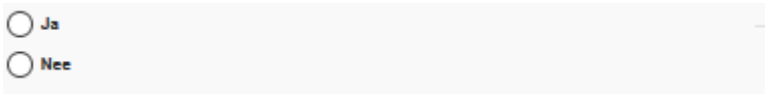

Stap 14 van 23
60%
Functies binnen de automatiseringsorganisatie
Het doel van deze vraag is inzicht te krijgen in de scheiding van functies in de automatiseringsorganisatie en een aantal daarmee samenhangende maatregelen.
Functioneert de automatiseringsafdeling onafhankelijk van de andere bedrijfsfuncties?
Toelichting functionering automatiseringsafdeling
Ja
Nee
Is het technisch beheer van systemen en applicaties gescheiden van het functioneel beheer?
Toelichting technisch beheer
Ja
Nee
Is er een helpdesk voor het registreren en oplossen van incidenten?
Toelichting helpdesk
Ja
Nee
Zijn er processen ingericht voor configuratiemanagement?
Toelichting processen configuratiemanagement
Ja
Nee
Is goedkeuren van wijzigingen in systemen/applicaties gescheiden van technisch en functioneel beheer?
Toelichting goedkeuren wijzigingen systemen
Ja
Nee
Is beheer van applicaties en systemen gescheiden van ontwikkeling van software?
Toelichting beheer applicaties/systemen
Ja
Nee
Zijn de automatiseringsafdeling en gebruikers functioneel gescheiden?
Toelichting automatiseringsafdeling
Ja
Nee


Stap 13 van 21
61%
Functie
Geef antwoord op onderstaande vragen m.b.t. functiescheiding automatiseringsprocessen en algemene procedures.
Functioneert de automatiseringsafdeling onafhankelijk van de andere bedrijfsfuncties?
Toelichting functionering automatiseringsafdeling
Ja
Nee
Is het technisch beheer van systemen en applicaties gescheiden van het functioneel beheer?
Toelichting technisch beheer
Ja
Nee
Is er een helpdesk voor het registreren en oplossen van incidenten?
Toelichting helpdesk
Ja
Nee
Zijn er processen ingericht voor configuratiemanagement?
Toelichting processen configuratiemanagement
Ja
Nee
Is goedkeuren van wijzigingen in systemen/applicaties gescheiden van technisch en functioneel beheer?
Toelichting goedkeuren wijzigingen systemen
Ja
Nee
Is beheer van applicaties en systemen gescheiden van ontwikkeling van software?
Toelichting beheer applicaties/systemen
Ja
Nee
Zijn de automatiseringsafdeling en gebruikers functioneel gescheiden?
Toelichting automatiseringsafdeling
Ja
Nee
Zijn financiële gegevensbestanden voor automatiseringspersoneel beveiligd tegen toegang?
Toelichting beveiliging financiële gegevensbestanden
Ja
Nee
Word de integriteit van data regelmatig gecontroleerd, bijvoorbeeld door verbandscontroles?
Toelichting integriteit data
Ja
Nee
Vorige
Volgende
Opslaan en later doorgaan


Stap 15 van 23
65%
Overzicht taken en functionarissen
Geef aan door welke functionaris (functie/groep) onderstaande taken worden uitgevoerd.
Door welke functionaris word technisch systeembeheer uitgevoerd?
Toelichting technisch systeembeheer
Door welke functionaris word technisch applicatiebeheer uitgevoerd?
Toelichting technisch applicatiebeheer
Door welke functionaris word netwerkbeheer uitgevoerd?
Toelichting netwerkbeheer
Door welke functionaris word functioneel applicatiebeheer uitgevoerd?
Toelichting functioneel applicatiebeheer
Door welke functionaris word databasemanagementbeheer uitgevoerd?
Toelichting databasemanagementbeheer
Als u aanvullende opmerkingen heeft of zaken wilt verduidelijken op dit onderdeel dan kunt u deze onderstaand aangeven.
Vorige
Volgende
Opslaan en later doorgaan

8. Werkwijze en procedures

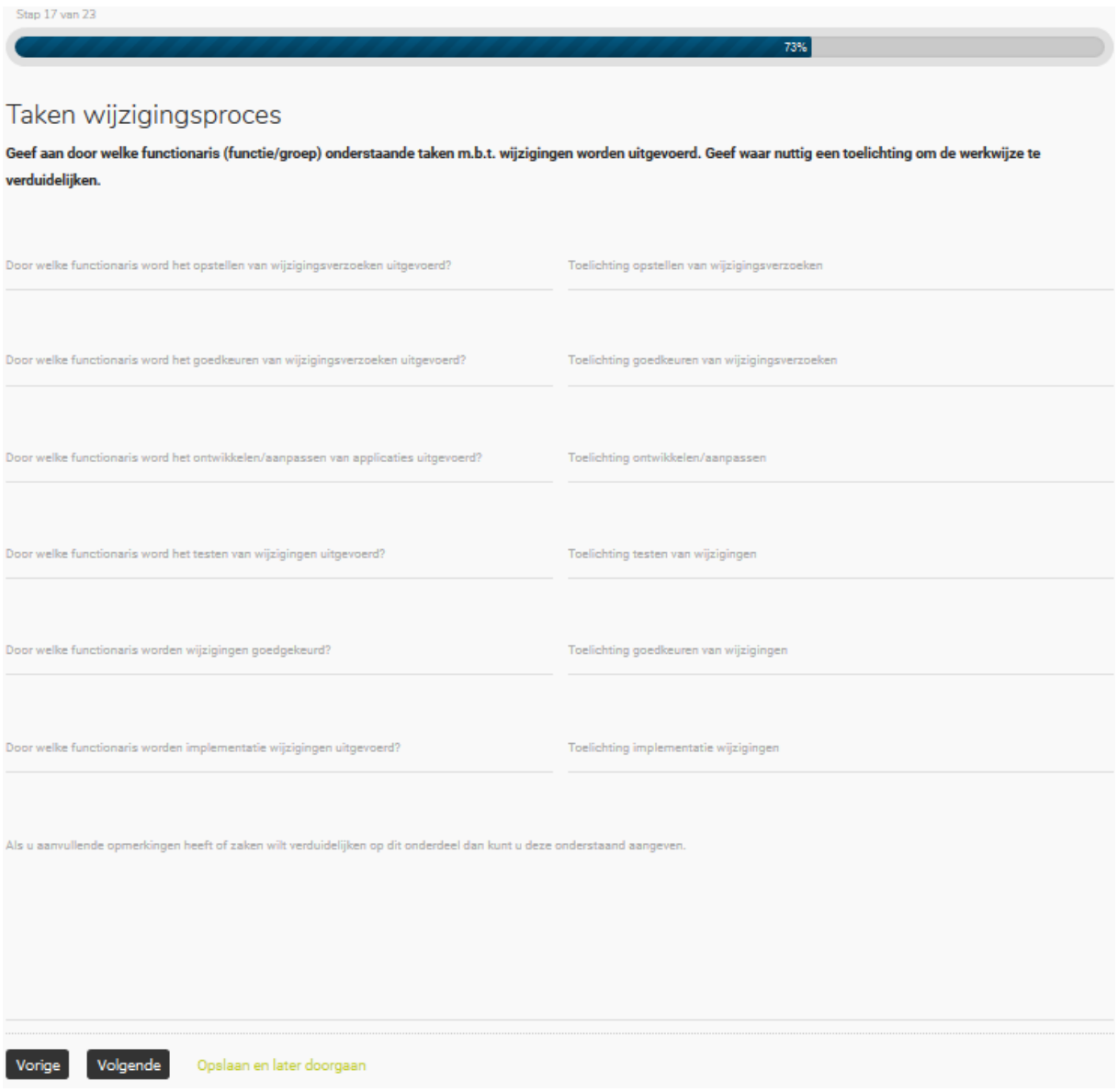
In dit onderdeel wordt gevraagd om op een aantal onderwerpen stellingen te antwoorden.
De stellingen/vragen in dit onderdeel kunt u beantwoorden door het antwoord van uw keuze te selecteren uit een van onderstaande antwoordopties:



Betekenis:
nee - aan de stelling/vraag wordt *niet* of *deels* voldaan
ja - aan de stelling/vraag wordt *geheel* voldaan

Bij elke stelling/vraag kunt u een ***korte*** toelichting geven. Deze toelichting kunt u bijvoorbeeld gebruiken om een afwijking op een 'volmondige' ja- of nee keuze nader toe te lichten.

**Als u meer ruimte nodig heeft voor de toelichting, kunt u deze opnemen in een afzonderlijk document. Hierbij adviseren wij u in de toelichting van de betreffende stelling/vraag een volgnummer of referentie op te nemen, waarnaar u in het document kunt verwijzen. Aan het eind van het assessment is een mogelijkheid opgenomen voor het elektronisch meesturen van een dergelijk document.*


Stap 17 van 23
73%
Taken wijzigingsproces
Geef aan door welke functionaris (functie/groep) onderstaande taken m.b.t. wijzigingen worden uitgevoerd. Geef waar nuttig een toelichting om de werkwijze te verduidelijken.
Door welke functionaris word het opstellen van wijzigingsverzoeken uitgevoerd?
Toelichting opstellen van wijzigingsverzoeken
Door welke functionaris word het goedkeuren van wijzigingsverzoeken uitgevoerd?
Toelichting goedkeuren van wijzigingsverzoeken
Door welke functionaris word het ontwikkelen/aanpassen van applicaties uitgevoerd?
Toelichting ontwikkelen/aanpassen
Door welke functionaris word het testen van wijzigingen uitgevoerd?
Toelichting testen van wijzigingen
Door welke functionaris worden wijzigingen goedgekeurd?
Toelichting goedkeuren van wijzigingen
Door welke functionaris worden implementatie wijzigingen uitgevoerd?
Toelichting implementatie wijzigingen
Als u aanvullende opmerkingen heeft of zaken wilt verduidelijken op dit onderdeel dan kunt u deze onderstaand aangeven.
Vorige
Volgende
Opslaan en later doorgaan

Stap 18 van 23

78%

Continuïteit

Beantwoord onderstaande stellingen m.b.t. continuïteit en licht de antwoorden eventueel toe.

Door het management zijn de eisen van beschikbaarheid vastgesteld.

- ◯ Ja
- ◯ Nee

Toelichting eisen beschikbaarheid

Een continuïteitsplan is beschikbaar.

- ◯ Ja
- ◯ Nee

Toelichting beschikbaarheid continuïteitsplan

Het continuïteitsplan voldoet aan de eisen van het management.

- ◯ Ja
- ◯ Nee

Toelichting voldoen continuïteitsplan

Het continuïteitsplan wordt periodiek getest.

- ◯ Ja
- ◯ Nee

Toelichting periodiek testen continuïteitsplan

Periodiek worden back-ups gemaakt.

- ◯ Ja
- ◯ Nee

Toelichting maken back-ups

De back-up cyclus is afgestemd op de eisen van het management.

- ◯ Ja
- ◯ Nee

Toelichting afgestemde back-ups

In de back-up cyclus is voorzien in de back-up van OS, applicaties en data.

- ◯ Ja
- ◯ Nee

Toelichting back-up cyclus

Back-ups worden op een externe locatie opgeslagen.

- ◯ Ja
- ◯ Nee

Toelichting back-up opslag

De geschiktheid van datadragers wordt periodiek gecontroleerd.

- ◯ Ja
- ◯ Nee

Toelichting datadragers

Kritische IT-middelen en personen zijn vastgesteld.

- ◯ Ja
- ◯ Nee

Toelichting kritische IT-middelen

De volgorde waarin systemen moeten worden hersteld, staat vast.

- ◯ Ja
- ◯ Nee

Toelichting herstel systemen

Herstelprocedures zijn formeel vastgesteld.

- ◯ Ja
- ◯ Nee

Toelichting formeel vaststellen herstelprocedures

Herstelprocedures worden regelmatig getest en geëvalueerd.

- ◯ Ja
- ◯ Nee

Toelichting testen herstelprocedures

Alle betrokken personen zijn geïnformeerd en getraind.

- ◯ Ja
- ◯ Nee

Toelichting betrokken personen

Als u aanvullende opmerkingen heeft of zaken wilt verduidelijken op dit onderdeel dan kunt u deze onderstaand aangeven.

Vorige Volgende Opslaan en later doorgaan

Stap 19 van 23

82%

Beveiliging

Beantwoord onderstaande stellingen m.b.t. beveiliging en licht de antwoorden eventueel toe.

De directie heeft formele richtlijnen vastgesteld.

- ◯ Ja
- ◯ Nee

Toelichting formele richtlijnen

De naleving van de richtlijnen wordt periodiek getoetst.

- ◯ Ja
- ◯ Nee

Toelichting naleving richtlijnen

Overtredingen worden gerapporteerd aan de directie.

- ◯ Ja
- ◯ Nee

Toelichting overtredingen

Systemen zijn beveiligd tegen onbevoegde toegang van buitenaf.

- ◯ Ja
- ◯ Nee

Toelichting beveiligde systemen

De netwerken en systemen zijn beveiligd tegen virussen, malware, spyware, trojan horses, DOS-aanvallen, etc.

- ◯ Ja
- ◯ Nee

Toelichting beveiliging netwerken en systemen

Voor de beveiliging van hulpmiddelen, die worden gebruikt voor de beveiliging, zijn procedures opgesteld.

- ◯ Ja
- ◯ Nee

Toelichting beveiliging van hulpmiddelen

Op de uitwisseling van gevoelige informatie zijn procedures van toepassing.

- ◯ Ja
- ◯ Nee

Toelichting procedures uitwisseling

Voor de controle op systeemlogs zijn procedures aanwezig.

- ◯ Ja
- ◯ Nee

Toelichting systeemlogs

Bij de locatie van de serverruimte is rekening gehouden met het belang van de ruimte.

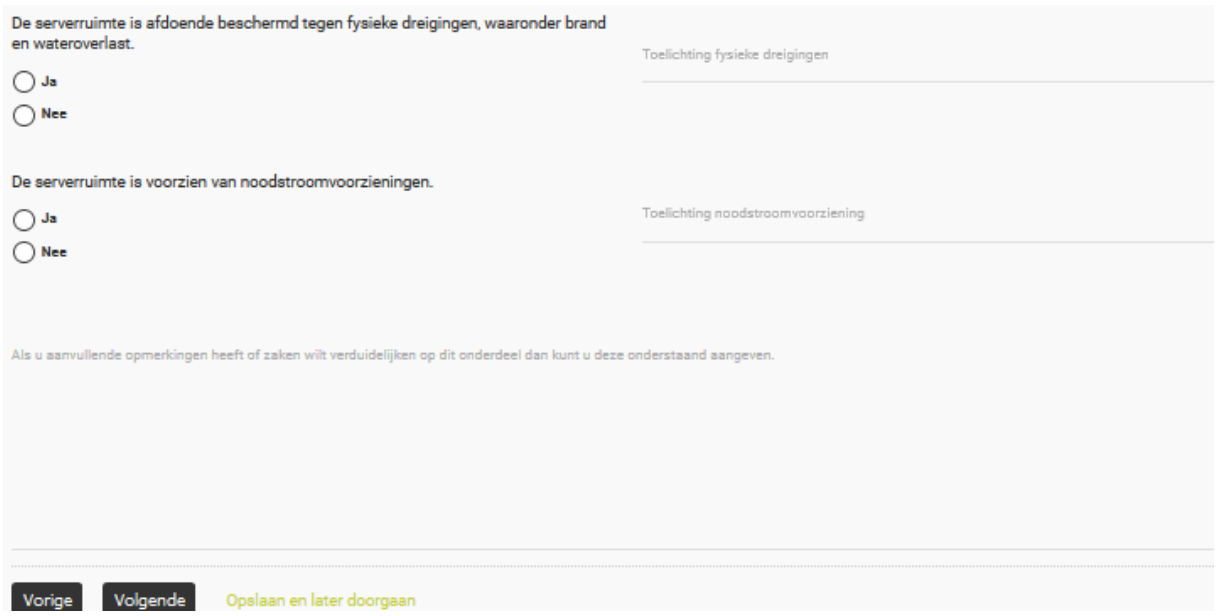
- ◯ Ja
- ◯ Nee

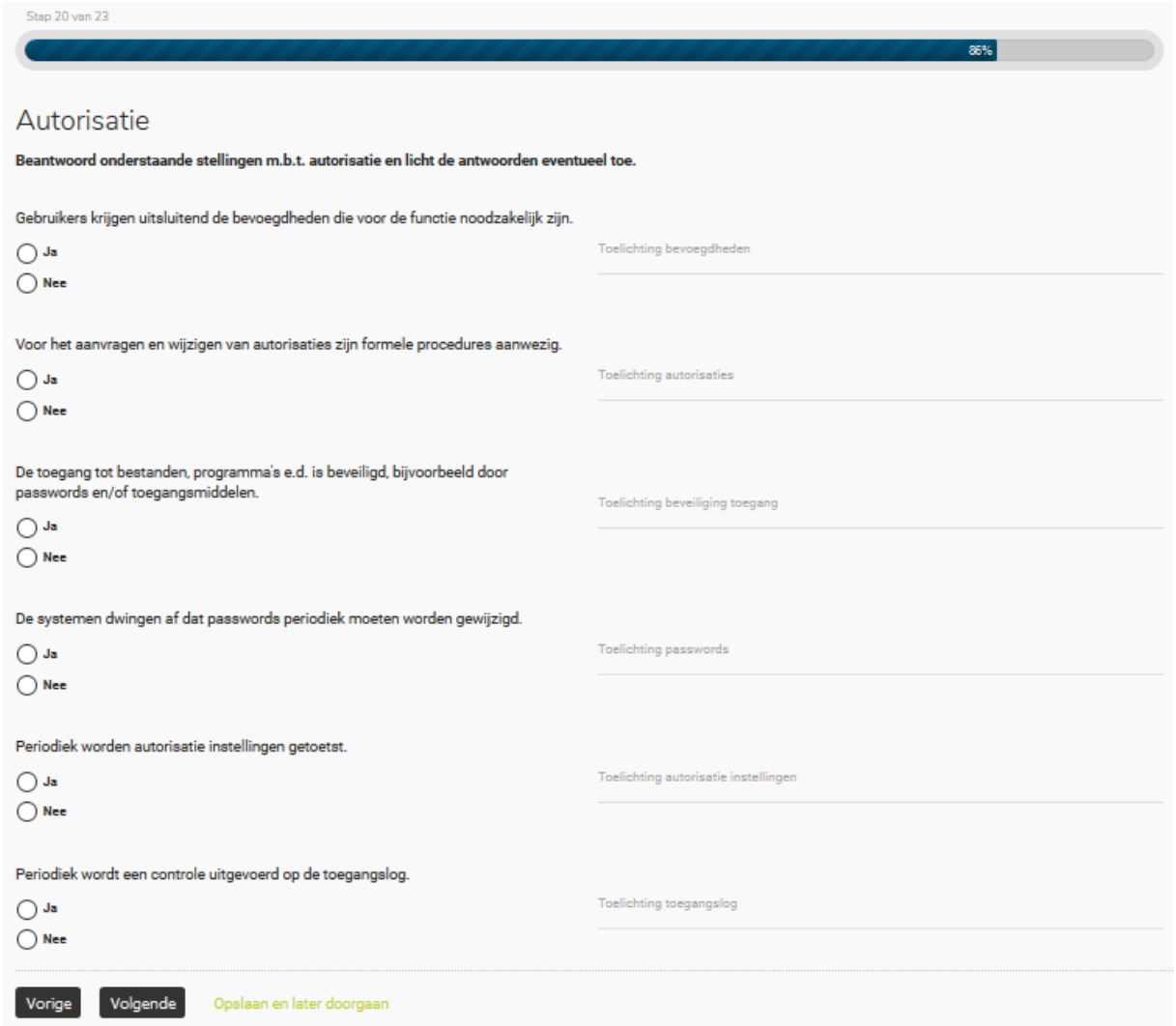
Toelichting locatie serverruimte

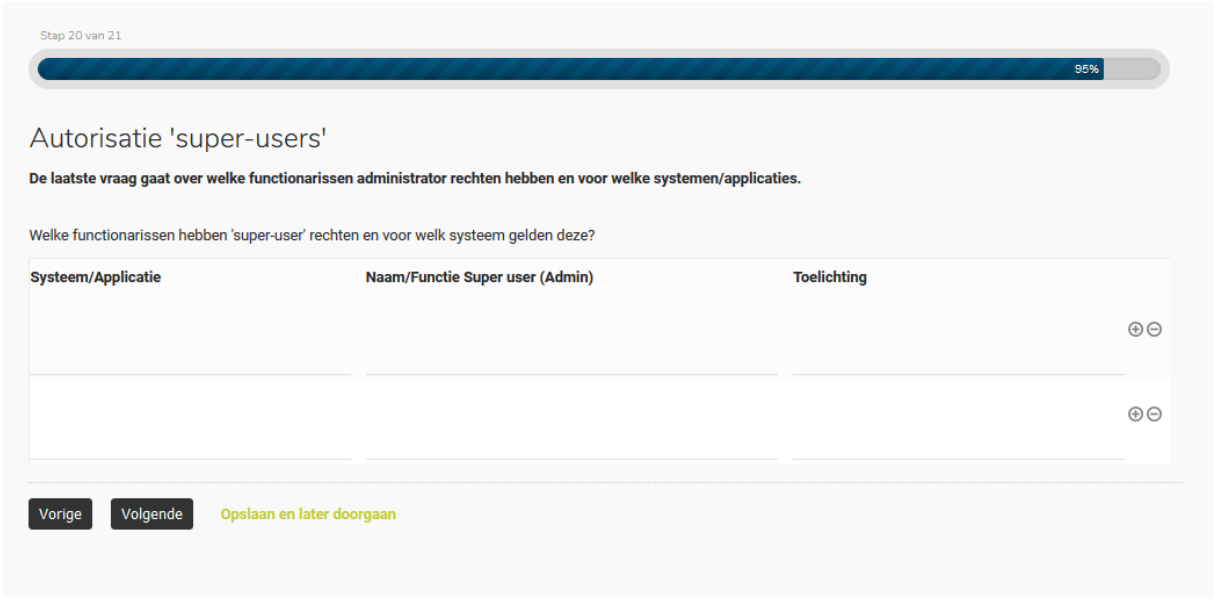
De fysieke toegang tot de serverruimte wordt beheerst.

- ◯ Ja
- ◯ Nee

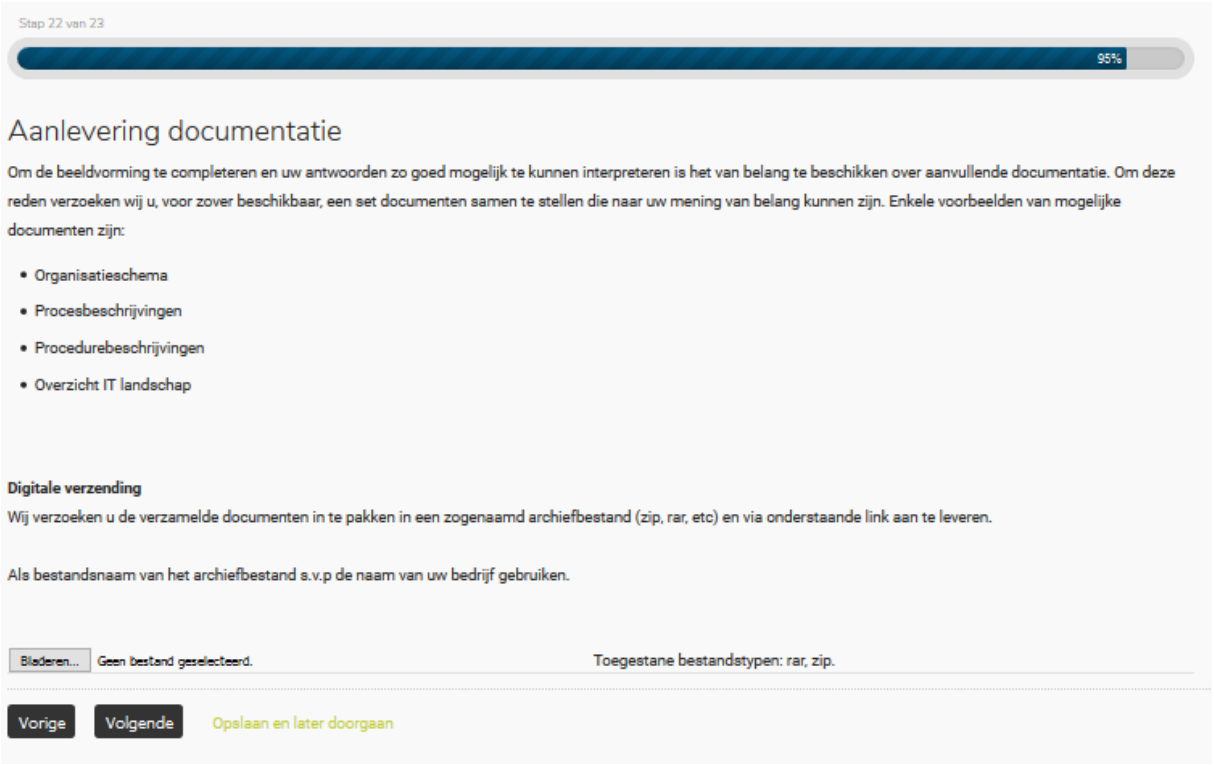
Toelichting fysieke toegang serverruimte


De serverruimte is afdoende beschermd tegen fysieke dreigingen, waaronder brand en wateroverlast.
Toelichting fysieke dreigingen
Ja
Nee
De serverruimte is voorzien van noodstroomvoorzieningen.
Toelichting noodstroomvoorziening
Ja
Nee
Als u aanvullende opmerkingen heeft of zaken wilt verduidelijken op dit onderdeel dan kunt u deze onderstaand aangeven.
Vorige
Volgende
Opslaan en later doorgaan


Stap 20 van 23
86%
Autorisatie
Beantwoord onderstaande stellingen m.b.t. autorisatie en licht de antwoorden eventueel toe.
Gebruikers krijgen uitsluitend de bevoegdheden die voor de functie noodzakelijk zijn.
Ja
Nee
Toelichting bevoegdheden
Voor het aanvragen en wijzigen van autorisaties zijn formele procedures aanwezig.
Ja
Nee
Toelichting autorisaties
De toegang tot bestanden, programma's e.d. is beveiligd, bijvoorbeeld door passwords en/of toegangsmiddelen.
Ja
Nee
Toelichting beveiliging toegang
De systemen dwingen af dat passwords periodiek moeten worden gewijzigd.
Ja
Nee
Toelichting passwords
Periodiek worden autorisatie instellingen getoetst.
Ja
Nee
Toelichting autorisatie instellingen
Periodiek wordt een controle uitgevoerd op de toegangslog.
Ja
Nee
Toelichting toegangslog
Vorige
Volgende
Opslaan en later doorgaan


Stap 20 van 21
95%
Autorisatie 'super-users'
De laatste vraag gaat over welke functionarissen administrator rechten hebben en voor welke systemen/applicaties.
Welke functionarissen hebben 'super-user' rechten en voor welk systeem gelden deze?
Systeem/Applicatie
Naam/Functie Super user (Admin)
Toelichting
Vorige
Volgende
Opslaan en later doorgaan

9. Aanlevering documentatie



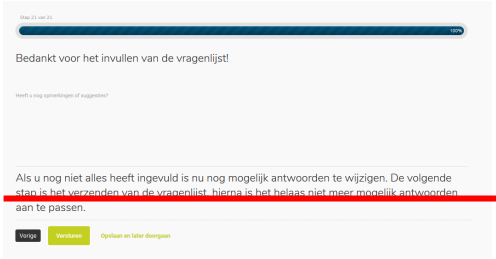
Button en link komen nog

10. Beëindigen assessment

Aan het einde van het assessment kunt u kiezen om:

- De ingevulde antwoorden te controleren en desgewenst nog te wijzigen;
- Het invullen te beëindigen en uw antwoorden te verzenden.

Versturen assessment
Als u zeker bent van de antwoorden, de aanvullende informatie hebt geselecteerd en eventueel een toelichting hebt gegeven kunt u het assessment versturen door op de knop versturen te klikken.



Daarmee wordt het assessment definitief gemaakt, verzonden naar onze database en kunnen de antwoorden niet meer worden gewijzigd. Daarna heeft u dan ook geen toegang meer tot de vragenlijst.

Per email ontvangt u vervolgens een opgave van de gegeven antwoorden voor uw eigen administratie.