

Uitwerkingen van de opdrachten bij  
IT-Service Management volgens ITIL

Peter Janssen

Pearson Education Benelux

ISBN 90-430-0676-9

## **Inhoudsopgave:**

<b>Toelichting op de antwoorden.....</b>	<b>3</b>
<b>Hoofdstuk 1 Ontwikkelingen in de IT .....</b>	<b>4</b>
<b>Hoofdstuk 2 Beheer van informatiesystemen .....</b>	<b>6</b>
<b>Hoofdstuk 3 Organisatie van het beheer .....</b>	<b>9</b>
<b>Hoofdstuk 4 Procesmatige aanpak van het beheer .....</b>	<b>11</b>
<b>Hoofdstuk 5 Servicedesk.....</b>	<b>14</b>
<b>Hoofdstuk 6 Configuration management.....</b>	<b>16</b>
<b>Hoofdstuk 7 Incident Management .....</b>	<b>19</b>
<b>Hoofdstuk 8 Problem Management.....</b>	<b>21</b>
<b>Hoofdstuk 9 Change Management .....</b>	<b>23</b>
<b>Hoofdstuk 10 Release Management.....</b>	<b>25</b>
<b>Hoofdstuk 11 Service Level Management.....</b>	<b>28</b>
<b>Hoofdstuk 12 Financial Management for IT-Services.....</b>	<b>30</b>
<b>Hoofdstuk 13 Availability Management .....</b>	<b>33</b>
<b>Hoofdstuk 14 Capacity Management .....</b>	<b>37</b>
<b>Hoofdstuk 15 IT Service Continuity Management .....</b>	<b>40</b>
<b>Hoofdstuk 16 Security Management .....</b>	<b>43</b>
<b>Hoofdstuk 17 Beheer door derden.....</b>	<b>46</b>
<b>Hoofdstuk 18 Relatie met andere standaarden .....</b>	<b>48</b>
<b>Hoofdstuk 22 Proefexamen 1: .....</b>	<b>51</b>
<b>Proefexamen 2 .....</b>	<b>52</b>

## **Toelichting op de antwoorden**

Dit document bevat de antwoorden die horen bij de opgaven uit het boek “IT-Service Management volgens Itil”, ISBN 90-430-0676-9, uitgegeven door Pearson Education Benelux. Per hoofdstuk uit het boek wordt achtereenvolgens een antwoordindicatie gegeven van de vragen en opdrachten bij de casus, de open vragen, de waar/niet waar vragen en de meerkeuzeopgaven. Ook worden de antwoorden van de beide modeexamens gegeven. Bij de antwoorden op de vragen bij de casussen hoort de kanttekening dat de casussen vooral bedoeld zijn voor discussie in de klas of in een groep. De verstrekte antwoorden moeten dan ook slechts worden gezien als een richtlijn. Naast de gegeven antwoorden zijn ook andere antwoorden mogelijk, dit ter beoordeling van de docent of de groep waarin de casussen worden besproken.

Naast de beide modeexamens achterin het boek kunnen tegen betaling andere modeexamens worden aangevraagd bij de stichting EXIN, de organisatie die in Nederland de Itil-examens afneemt. De modeexamens kunnen telefonisch (030-2344811) of via de website van EXIN ([www.exin.nl](http://www.exin.nl)) worden aangevraagd. Deze antwoordindicatie en het boek zijn met de grootste zorg samengesteld. Het is echter onvermijdelijk dat er zowel in het boek als in de antwoordindicatie fouten staan. Docenten en studenten worden verzocht deze fouten te melden bij de auteur, liefst via email: [pjsjans@hotmail.com](mailto:pjsjans@hotmail.com), zodat deze bij een herdruk kunnen worden verbeterd en andere docenten en studenten nóg prettiger met het boek zullen werken.

Amsterdam, 26 januari 2004

Peter Janssen

## Hoofdstuk 1 Ontwikkelingen in de IT

### Vragen en opdrachten met betrekking tot de casus:

1. Een IBM-pc, een database, procedures en medewerkers
2. Centraal: de medewerkers maken gebruik van één IBM-pc.
3. Nu worden de gegevens decentraal verwerkt, op verschillende computers met op elke computer een kopie van het klantenbestand
4. Installeren van computers en programma's (Windows en Office), installeren van het klantenbestand, oplossen van storingen.
5. De vraag naar beheer is toegenomen, door de toename van het aantal pc's en de toename van het aantal beheertaken.
6. De wijzigingen in het klantenbestand worden niet centraal, op één plek bijgehouden, waardoor er op den duur verschillende versies van het klantenbestand ontstaan.
7. Nee, het beheer neemt alleen maar toe en wordt als gevolg daarvan steeds duurder.
8. Een urenregistratie bijhouden, waardoor duidelijk wordt hoeveel tijd er nodig is voor de verschillende beheertaken.
9. Zorgen dat er meer structuur komt in het beheer: één centraal klantenbestand gebruiken, zorgen dat de systemen stabiel worden, de gebruikers op cursus sturen, zodat ze beter met de programma's overweg kunnen.
10. Maatregelen: één centraal aanspreekpunt voor alle storingsmeldingen invoeren, één centraal klantenbestand gebruiken, de gebruikers beter opleiden.

### Open vragen:

1. De hardware werd sneller, kleiner, stabiel, gebruikersvriendelijker en goedkoper.
2. Het weefgetouw is een apparaat dat instructies kan verwerken die met behulp van gaatjes in plankjes. De plankjes met gaten bevatten programma-instructies en gegevens.
3. De eerste generatie computers kon alleen maar rekenen, de huidige computers zijn multifunctioneel en veel sneller, kleiner, stabiel, gebruikersvriendelijker en goedkoper dan de computers van de eerste generatie.
4. Een geautomatiseerd informatiesysteem heeft tot doel het verwerken van gegevens tot informatie; de onderdelen zijn: apparatuur, programmatuur, gegevensverzamelingen, procedures en mensen.
5. De eerste computers konden alleen rekenen, vanaf begin 1960 is de computer ook in staat om grote hoeveelheden administratieve gegevens te verwerken.
6. Centraal betekent dat de gegevens op één plek worden verwerkt, de gegevens die de gebruikers vanaf hun werkplek invoeren worden op één plek verwerkt. Een standalone-pc wordt vooral decentraal gebruikt, de gegevens worden op verschillende plekken ingevoerd en verwerkt.
7. Het rekencentrum beheert de centraal opgestelde informatiesystemen.
8. Bij decentrale computersystemen was in het begin niet duidelijk wie er verantwoordelijk was voor het beheer, zodat de gebruikers dat zelf gingen doen. Een ander probleem is dat het beheer complexer wordt, omdat de decentrale computers op verschillende plekken staan, waardoor het rekencentrum er geen zicht meer op heeft. Tevens hebben de gebruikers te weinig kennis van het beheer van hun informatiesystemen, wat ten koste gaat van de stabiliteit.
9. Het rekencentrum kreeg er steeds meer beheertaken bij door de toename van de hoeveelheid, de verscheidenheid, de spreiding en de complexiteit van de gebruikte informatiesystemen.
10. Een centrale computer is over het algemeen beter te beheren, omdat alle inspanningen van het beheer zich kunnen concentreren op één plek.

**Waar/niet waar:**

1. Niet waar
2. Waar
3. Waar
4. Waar
5. Waar
6. Waar
7. Niet waar, het doel is gegevensverwerking
8. Waar
9. Waar
10. Waar

**Meerkeuzeopgaven:**

1. D
2. B
3. B
4. A, gegevens wél!
5. C
6. A

## Hoofdstuk 2 Beheer van informatiesystemen

### Vragen en opdrachten met betrekking tot de casus:

1. Apparatuur: de unix-server; programmatuur: het informatiesysteem BIS; gegevensverzamelingen: de gegevens over fietsvakanties en klanten; mensen: Jaap en zijn collega's van de afdeling automatisering; procedures: de manier waarop de gebruikers gebruik kunnen maken van het BIS.
2. Het reële systeem zijn bij Bikefun de primaire bedrijfsprocessen als het verhuren van fietsen, het verkopen van fietsvakanties, het reserveren van fietsvakanties, het vervoer van personen en fietsen. Het informatiesysteem is BIS, een combinatie van apparatuur, programmatuur, gegevens, mensen en procedures.
3. Beheer: de taken die Jaap en zijn collega's van de afdeling automatisering uitvoeren met betrekking tot de instandhouding van het BIS. Exploitatie: de taken die Jaap en zijn collega's van de afdeling automatisering uitvoeren met betrekking tot het operationeel houden van het BIS en de taken die ze uitvoeren om ervoor te zorgen dat het BIS van nut is bij het uitvoeren van de bedrijfsdoelstellingen. Onderhoud: de twee ontwikkelaars die op verzoek van de gebruikers het BIS regelmatig wijzigen of aanpassen.
4. De besturing van de bedrijfsprocessen van Bikefun vindt plaats door het informatiesysteem BIS, dat daarvoor nauw samenwerkt met het reële systeem. Het informatiesysteem BIS ontvangt daarvoor informatie vanuit de bedrijfsprocessen van Bikefun en vanuit de omgeving (wetten en voorschriften van de overheid).
5. Vanuit de gebruikers van Bikefun worden er allerlei eisen gesteld aan het BIS. Ook het management stelt eisen en randvoorwaarden aan het gebruik van het BIS. Vanuit het beheer moeten er activiteiten worden uitgevoerd om het gebruik te laten plaatsvinden overeenkomstig de eisen en randvoorwaarden.
6. Bestuurlijke invloeden: veranderingen in de bedrijfsprocessen van Bikefun; informatische invloeden: wijzigingen in de wet; bedrijfseconomische invloeden: wijzigingen in de economische situatie; technische invloeden: ontwikkelingen in de techniek. Al deze invloeden kunnen aanleiding geven tot aanpassingen in het reële systeem of in het informatiesysteem.
7. Recursiebeginsel bij het informatieparadigma: elk reëel systeem en elk informatiesysteem bestaan uit deelsystemen, die op hun beurt weer zijn opgebouwd uit een reëel systeem en een informatiesysteem. Recursiebeginsel bij het beheerparadigma: ook het beheer heeft een informatiesysteem nodig om voor de besturing van haar eigen reëel systeem. Dit beheer-informatiesysteem moet ook weer beheerd worden etc.
8. IBP: de toestand voorafgaand aan het BIS, waarin bij Bikefun nagedacht werd over het informatiebeleid. In toestand O wordt het informatiesysteem BIS ontworpen en gebouwd, in toestand AI wordt het informatiesysteem door de gebruikers geaccepteerd en ingevoerd. In toestand G wordt het systeem gebruikt, in toestand E wordt het BIS operationeel gehouden en in toestand W worden wijzigingen doorgevoerd.
9. Toestand IBP: volgen van de technische ontwikkeling. Toestand O: advies geven aan de ontwikkelaars met betrekking tot de wensen van de gebruikers. Toestand AI: controleren of gebruik en beheer voldoende zijn ingericht om met het nieuwe systeem om te kunnen gaan. Toestand G: ondersteuning van de gebruikers die met het systeem werken. Toestand E: inspelen op technologische en bedrijfseconomische ontwikkelingen. Toestand W: wijzigen van het informatiesysteem als gevolg van fouten in de programmatuur.
10. Correctief onderhoud: het herstellen van fouten in het BIS. Preventief onderhoud: het voorkomen van fouten in het BIS. Perfectief onderhoud: het verbeteren van de prestaties van het BIS. Adaptief onderhoud: aanpassingen van het informatiesysteem vanwege

veranderingen in de voorschriften van de overheid. Additief onderhoud: aanpassingen in het BIS als gevolg van de gewijzigde functionele eisen.

**Open vragen:**

1. Het geheel van apparatuur, met bijbehorende basisprogrammatuur en toepassingsprogrammatuur, gegevensverzamelingen, procedures en personen voor het kennen, besturen en ondersteunen van reële systemen.
2. Apparatuur, programmatuur, gegevensverzamelingen, mensen en procedures.
3. Technische infrastructuur, technische gegevensinfrastructuur, applicatie-infrastructuur en informatie-infrastructuur.
4. zie vraag 1
5. Informatievoorziening is het geheel aan activiteiten dat binnen een organisatie moet worden uitgevoerd om iedereen te voorzien van de informatie die nodig is voor de vervulling van de toegewezen functies.
6. De eigenaar van een informatiesysteem is verantwoordelijk voor de functionaliteit van het informatiesysteem. De gebruikers van een informatiesysteem zijn de mensen die voor hun werkzaamheden gebruik maken van de functionaliteit van een informatiesysteem.
7. Exploitatie is het operationeel houden van het informatiesysteem. Onderhoud wil zeggen het aanbrengen van wijzigingen in het informatiesysteem. Beheer wil zeggen het instandhouden van het informatiesysteem overeenkomstig de eisen en randvoorwaarden vanuit het gebruik.
8. Correctief, preventief, perfectief, adaptief en additief onderhoud.
9. Het informatiesysteem is nodig voor de ondersteuning en besturing van het reële systeem, de bedrijfsprocessen van een organisatie.
10. Informatieparadigma: voor de besturing en ondersteuning van de bedrijfsprocessen van een organisatie is een informatiesysteem nodig.
11. Beheerparadigma: Voor het beheer van het informatiesysteem is een beheerafdeling nodig, waarbij alle onderdelen van het beheerparadigma (reëel systeem, informatiesysteem en beheer) worden beïnvloed door informatische, bestuurlijke, bedrijfseconomische en technische invloeden.
12. Informatische, bestuurlijke, bedrijfseconomische en technische invloeden.
13. Het recursiebeginsel bij zowel het informatieparadigma als het beheerparadigma houdt in dat beide paradigma ook gelden voor deelsystemen, met andere woorden de beheerafdeling heeft weer een eigen informatiesysteem nodig voor de besturing van haar eigen reële systeem.
14. Het toestandenmodel brengt de verschillende toestanden van een informatiesysteem gedurende de levensloop van dat informatiesysteem in kaart en plaatst daarin de verschillende beheertaken.
15. IBP: informatiebeleid en -planning; O: ontwikkeling; AI: acceptatie en invoering; G: gebruik, E: exploitatie; W: wijzigen.
16. Toestand IBP: volgen van de technische ontwikkeling. Toestand O: advies geven aan de ontwikkelaars met betrekking tot de wensen van de gebruikers. Toestand AI: controleren of gebruik en beheer voldoende zijn ingericht om met het nieuwe systeem om te kunnen gaan. Toestand G: ondersteuning van de gebruikers die met het systeem werken. Toestand E: inspelen op technologische en bedrijfseconomische ontwikkelingen. Toestand W: wijzigen van het informatiesysteem als gevolg van fouten in de programmatuur.
17. Het uitgebreid toestandenmodel geeft het voortschrijdend karakter in de tijd en de consequenties die daaraan zijn verbonden voor het beheer beter in kaart.
18. Correctief, preventief, perfectief, adaptief en additief onderhoud.

**Waar/niet waar:**

1. Waar
2. Waar
3. Niet waar: architectuur, uitrusting en realisatie.
4. Niet waar: de applicatie-infrastructuur bestaat uit de toepassingsprogrammatuur en de bijbehorende gegevensverzamelingen.
5. Niet waar, het doel van informatievoorziening is iedereen van de juiste informatie te voorzien.
6. Niet waar, de gebruiker maakt gebruik van de functionaliteit, de eigenaar is verantwoordelijk voor de functionaliteit.
7. Waar, beheer bestaat uit exploitatie en onderhoud.
8. Waar
9. Waar
10. Waar, zie figuur 2.2
11. Waar
12. Niet waar
13. Waar
14. Waar
15. Waar
16. Waar

**Meerkeuzeopgaven:**

1. D
2. D
3. A
4. A
5. D
6. B
7. B
8. B, dit is geen toestand waarin het IS zich kan bevinden.
9. A, bij het bepalen van het informatiebeleid wordt rekening gehouden met de bestaande IS.
10. C



### **Hoofdstuk 3 Organisatie van het beheer**

#### **Vragen en opdrachten met betrekking tot de casus:**

1. Jaap: management, managen van de personele aspecten, gebruiksbeheer;  
José: functioneel onderhoud en applicatieonderhoud;  
Hans: technische ondersteuning, onderhoud technische infrastructuur en operationele ondersteuning;  
Jerrold: functioneel onderhoud en applicatieonderhoud;  
Abdel: technische ondersteuning, onderhoud technische infrastructuur en operationele ondersteuning;
2. Zie tabel bladzijde 46 t/m 48.
3. José: functioneel beheer; Jaap en Jerrol: applicatiebeheer; Hans en Abdel: technisch beheer.
4. Technisch beheer: Hans en Abdel verzorgen het operationele aspect.  
Functioneel beheer: José verzorgt het operationele aspect.  
Applicatiebeheer: Jaap verzorgt het strategische aspect, Jerrol het operationele.  
De andere aspecten worden niet duidelijk ingevuld.
5. Doel: probleem oplossen. Volgorde van taken: bijvoorbeeld aannemen, registreren, categoriseren, opzoeken, analyseren, diagnosticeren, oplossen, herstellen, administreren.
6. Uit de casus blijken in ieder geval de volgende taakclusters: beheren prestatiekenmerken applicatie, beheren functionaliteit applicatie, bepalen onderhoud op applicaties, uitvoeren onderhoud op applicaties, beheren netwerk, beheren netwerkanapplicaties, beheren prestatiekenmerken netwerk, beheren beschikbaarheid van gegevens, beheren productieomgeving, oplossen systeemstoringen en incidenten, ondersteunen gebruiker bij gebruik component.
7. Functioneel en technisch applicatiebeheerder, systeembeheerder, netwerkbeheerder, pc-beheerder.

#### **Open vragen:**

1. Eisen vanuit het gebruik, randvoorwaarden vanuit het gebruik, karakteristieken van apparatuur, karakteristieken van programmatuur, karakteristieken van gegevensverzamelingen, karakteristieken van procedures en karakteristieken van mensen.
2. Eisen vanuit het gebruik: snelheid en gebruikersgemak, randvoorwaarden vanuit het gebruik: controlemogelijkheden voor de gebruikers, karakteristieken van apparatuur: de hoeveelheid geheugen in de pc, karakteristieken van programmatuur: soort besturingssysteem, karakteristieken van gegevensverzamelingen: aantal bestanden en velden, karakteristieken van procedures: back-up en inloggen, karakteristieken van mensen: kennis en ervaring.
3. Technisch beheer, applicatiebeheer en functioneel beheer.
4. Zie figuur 3.2 op bladzijde 49.
5. Functioneel beheer richt zich op de instandhouding van de functionaliteit van het informatiesysteem.
6. Ja.
7. Technisch beheer is verantwoordelijk voor de instandhouding van de operationalisering van het informatiesysteem.
8. De drie beheereenheden moeten samenwerken om problemen met informatiesystemen op te lossen.
9. Binnen de ontwikkelomgeving spelen zaken als versiebeheer en de gebruikte methoden en technieken een centrale rol. Binnen de exploitatieomgeving spelen de performance en stabiliteit van het informatiesysteem een centrale rol.

10. Met behulp van het logo van Mintzberg kunnen de drie managementniveaus (strategisch, tactisch en operationeel) van het beheer binnen de drie beheereenheden (functioneel-, technisch- en applicatiebeheer) worden weergegeven.
11. In het uitgebreid drievoudig model van beheer kan elke beheervorm vaker dan eenmaal voorkomen. Binnen elke beheervorm worden de taakgebieden vermeld. Vervolgens worden clusters van beheertaken gevormd, die op zijn te vatten als een aantal bij elkaar behorende beheertaken dat goed herkenbaar is. In het onderste gedeelte van het model worden uit de gevormde clusters van beheertaken die beheertaken geselecteerd, die voor de uitvoering van een bepaald beheerproces in aanmerking komen.
12. Kritische, in gedragstermen omschreven kenmerken van mensen die ten grondslag liggen aan succesvol functioneren binnen een organisatie.
13. Analytisch vermogen, creativiteit, methodisch werken, accuratesse.

**Waar/niet waar:**

1. Waar
2. Waar
3. Waar
4. Niet waar
5. Waar
6. Waar
7. Waar
8. Waar
9. Waar
10. Waar

**Meerkeuzeopgaven:**

1. B
2. A
3. C
4. A
5. B
6. C
7. B
8. C
9. D
10. C

## Hoofdstuk 4 Procesmatige aanpak van het beheer

### Vragen en opdrachten met betrekking tot de casus:

1. Klant: degene die namens de gebruikers van Bikefun afspraken maakt met de IT-afdeling.  
Gebruiker: de medewerkers van Bikefun die voor hun dagelijkse werkzaamheden gebruik maken van BIS.
2. Nee, de medewerkers van de IT-afdeling zijn vaak niet bereikbaar.
3. Visie: klantgericht werken, missie: de klant is koning, doelen: beschikbaarheid van 99%, performanceverbetering, centrale melding van storingen, maken van functiebeschrijvingen, taakverdeling, en dat alles volgens het SMART-principe.
4. De kwaliteit van BIS is slecht: veel storingen, lage beschikbaarheid en performance.
5. De kwaliteit van de IT-afdeling is ook minimaal: medewerkers zijn niet bereikbaar, hebben niet voldoende kennis, oplossen van storingen kost veel tijd, er is geen centrale incidentenregistratie, medewerkers werken lang elkaar heen, er is geen verdeling van taken en verantwoordelijkheden en het is niet duidelijk wat ieders functie is.
6. Eerst een plan van aanpak opstellen voor de IT-afdeling, vervolgens de plannen uitvoeren, vervolgens controleren of de doelen zijn gehaald, en indien nodig de plannen aanpassen.
7. Maak een plan voor een standaardwerkwijze. Voer het plan vervolgens uit. Controleer of de werkwijze goed is. Stel het plan zonnodig bij en voer de stappen opnieuw uit.
8. Proces: storingsafhandeling. Doel: zo snel mogelijk oplossen van de storing. Activiteiten: storingsmelding, registratie, inschatten van prioriteit, telefonisch oplossen, doorsturen naar specialist, sluiten en registratie bijwerken.
9. Centrale melding en registratie van storingen, aanleggen van een registratie met de meest voorkomende storingen en oplossingen, vergroten van de kennis van de medewerkers.
10. Eerst een nulmeting bij aanvang en daarna periodiek meten van: aantal storingen, duur van de storing, oplospercentage via de telefoon, aantal keren dat storingen terug komen.
11. Centrale helpdesk, duidelijke verdeling van taken en verantwoordelijkheden, snel opnemen van de telefoon, snelle oplossing van storingen, accurate oplossing van storingen.
12. Bikefun moet een cultuurverandering ondergaan, er moet meer procesgericht en businessgericht worden gewerkt, waarbij de doelen van de organisatie voorop komen te staan. Ook moet het management vanaf het begin bij de invoering van ITIL worden betrokken en haar betrokkenheid tonen bij de invoering ervan.
13. De cultuurverandering die gepaard gaat met de invoering van ITIL roept weerstanden op, onvoldoende betrokkenheid bij het management, te ambitieuze planning, medewerkers proberen de procedures, die als bureaucratisch worden ervaren te omzeilen, de verbetering van de dienstverlening moet zichtbaar worden gemaakt door te beginnen met een nulmeting.

**Open vragen:**

1. Doordat veel organisaties gebruik maken van Itil, is een standaard ontstaan voor het invullen van de technische beheerprocessen waar veel organisaties vrijwillig aan voldoen.
2. 1 The Business Perspective: het zakelijke perspectief; 2 Supporting IT Services: ondersteuning van IT-diensten; 3 Delivering IT Services: levering en planning van IT-diensten; 4 Managing Applications: applicatiebeheer; 5 Managing the Infrastructure: beheren van de infrastructuur.
3. De stukjes van de puzzel passen niet precies in elkaar, maar schuiven als ijsschotsen over elkaar en overlappen elkaar gedeeltelijk. Zo verschuift het zakelijke perspectief voortdurend, moeten er steeds andere IT-diensten worden ondersteund en geleverd en gepland en veranderen de applicaties en de infrastructuur voortdurend, waardoor andere diensten ondersteund moeten worden.
4. Klantgerichte benadering, procesmatige aanpak, public-domain gedachte, best practice.
5. IT Service Management stelt de klant centraal en gaat uit van een kwalitatief hoogstaande dienstverlening die voorziet in de behoeften van de klant.
6. De gebruiker van een IT-dienst is degene die voor zijn werkzaamheden gebruik maakt van deze dienst, de klant is degene die bevoegd is om namens de gebruikers van IT-diensten afspraken te maken over de inhoud en het niveau van de dienstverlening met de IT-afdeling.
7. Bij een procesmatige aanpak ligt de nadruk op het doel van de de beheerprocessen, en niet op de functies en afdelingen, waardoor veel beter inzicht kan worden verkregen in de activiteiten die moeten worden uitgevoerd om een bepaalde taak te vervullen.
8. Bij de beschrijving van een proces (wat moet worden gedaan?) maken we gebruik van procedures (wie doet wat?) en werkinstructies (hoe wordt het gedaan?).
9. De medewerkers van de organisatie hebben een gezamenlijke visie op de klanten en de buitenwereld en handelen vanuit een bepaald idee over waarom het de moeite waard is om bij juist bij deze organisatie te werken. Deze visie moet naar buiten toe duidelijk worden gemaakt. De klanten, aandeelhouders en andere belanghebbenden willen weten waarom ze nou juist bij deze organisatie moeten zijn voor een bepaald artikel of dienst. Deze visie van de organisatie kan worden uitgedragen in een missie of mission statement. Vervolgens kan deze missie concreet worden gemaakt door het benoemen van concrete doelstellingen. Deze doelstellingen beschrijven in concrete termen wat de organisatie wil bereiken. Om de doelstellingen concreet te maken en te realiseren, ontwikkelt een organisatie beleid. Het beleid geeft aan hoe de doelen van een organisatie moeten worden bereikt.
10. Goede doelstellingen zijn Specifiek (geven aan wat de medewerkers willen bereiken), Meetbaar (zodat getoetst kan worden of ze worden gehaald), Acceptabel (ze moeten door alle medewerkers worden onderschreven), Realistisch (ze moeten kunnen worden gehaald) en Tijdgebonden (ze moeten binnen de afgesproken tijd worden gehaald).
11. Door de stappen uit het procesverbeteringsmodel uit te voeren: bij elk proces vragen we ons af wat er moet gebeuren, welke resultaten we verwachten en hoe de resultaten van de processen elkaar beïnvloeden. Op verschillende plaatsen in de processen worden meetpunten ingelast om te meten of het doel al bereikt is. Elk proces heeft een procesverantwoordelijke of proceseigenaar die er op toeziet of het doel wordt bereikt en bijstuurt indien nodig.
12. Het geheel van eigenschappen en kenmerken van een product of dienst dat van belang is voor het voldoen aan vastgestelde of vanzelfsprekende behoeften.
13. Eerst wordt een planning gemaakt: wie doet wat, waar en wanneer?; vervolgens wordt de planning uitgevoerd: het uitvoeren van de geplande activiteiten; daarna controleren: meten

of het geplande wordt gehaald; tenslotte wordt de planning aangepast: de plannen worden bijgesteld.

14. De organisatie moet een cultuurverandering ondergaan en het management moet bij de invoering worden betrokken.
15. De organisatie zal moeten wennen aan de klantgerichte benadering van ITIL. De gebruikers en de medewerkers van de IT-afdeling moeten meer procesgericht en businessgericht gaan werken. De klant/leverancierrelatie komt centraal te staan.
16. Voorlichting, betrokkenheid van het management en die ook uitdragen, cursussen, in het begin een aantal successen inbouwen en die uitgebreid vieren.
17. Verbeterde dienstverlening, duidelijker afspraken, duidelijke communicatielijnen, toegenomen tevredenheid van de gebruikers en de medewerkers van de IT-afdeling, de mogelijkheid om de kwaliteit van de dienstverlening voortdurend te meten en bij te sturen, hogere productiviteit, minder uitval van bedrijfsprocessen door storingen, meer inzicht in de kosten van de IT-dienstverlening.
18. Weerstanden, door de cultuurverandering, geen betrokkenheid bij het management, te ambitieuze planning, omzeilen van procedures, resultaten worden onvoldoende zichtbaar gemaakt.

**Waar/niet waar:**

1. Niet waar
2. Niet waar
3. Waar
4. Waar
5. Niet waar
6. Niet waar
7. Niet waar
8. Niet waar
9. Waar
10. Niet waar
11. Niet waar
12. Niet waar
13. Niet waar
14. Waar
15. Waar

**Meerkeuzeopgaven:**

1. B
2. A
3. A
4. C
5. B
6. B
7. D
8. B
9. B
10. D
11. D
12. A
13. C

## Hoofdstuk 5 Servicedesk

### Vragen en opdrachten met betrekking tot de casus:

1. Hoge werkdruk, ziekteverzuim, veel storingen aan het BIS, onvoldoende verdeling van taken en verantwoordelijkheden, waardoor de verkeerde mensen erop uit worden gestuurd om een storing op te lossen.
2. Ja, door de storingen centraal te melden en registreren, kan een betere afweging worden gemaakt wie een bepaalde storing op moet lossen, waardoor tijd wordt gewonnen en de ergernis en onmacht van de IT-medewerkers afneemt.
3. Voornamelijk configuratiebeheer, incidentbeheer en probleembeheer, aangevuld met delen van de andere processen.
4. Voorlichting geven, cursussen geven, informatie verstrekken, nieuwsbrieven rondsturen etc.
5. Centraal, het is een kleine organisatie waardoor een centrale servicedesk het meest efficiënt is.
6. Fax, e-mail, voice respons, ACD, SMS, CTI en VOIP, zie blz. 85-86.
7. Skilled, om te proberen de andere IT-medewerkers te ontlasten door oplossingen van storingen te documenteren.
8. Klantvriendelijkheid, goed kunnen luisteren, in een team kunnen werken.
9. Beantwoorden van vragen, problemen en verzoeken om informatie, registratie van storingen, bewaken van de voortgang van storingen, aansturen van leveranciers, operationele beheerstaken als het maken van backups of het resetten van passwords.
10. Rapportages over de tevredenheid van de gebruikers, aantal opgeloste storingen, aantal calls per werkplek en de gemiddelde tijd per call.

### Open vragen:

1. Configuratiebeheer, incidentenbeheer, probleembeheer, wijzigingsbeheer, uitgavenbeheer, beheer van de relaties met de klant, lokaal beheer, dienstenniveaubehoor.
2. Reactief beheer komt pas in actie als een storing wordt gemeld, proactief beheer probeert problemen te voorkomen door het geven van voorlichting, instructie enz.
3. De servicedeskmedewerker registreert alle binnenkomende storingen en probeert de dienstverlening aan de gebruiker zo snel mogelijk te herstellen.
4. De servicedesk verleent de tussen de IT-afdeling en de gebruiker overeengekomen dienstverlening door de bereikbaarheid en toegankelijkheid van de IT-afdeling te garanderen.
5. Het snel verhelpen van simpele storingen; het verzorgen van voorlichting aan de gebruikers; de installatie van standaard soft- en hardware; de registratie van soft- en hardware; het in ontvangst nemen van wijzigingsverzoeken; het ondersteunen van de gebruikers bij hun werk.
6. Fax, e-mail, voice respons, ACD, SMS, CTI en VOIP, zie blz. 85-86.
7. Bij een centrale servicedesk functioneert de servicedesk als centraal aanspreekpunt voor de gebruikers en is ook fysiek op één plek gehuisvest. Bij een gedistribueerde servicedesk zijn er verschillende servicedesks ingericht binnen de organisatie, die ook fysiek op verschillende plekken zijn gehuisvest.
8. Door gebruik te maken van moderne communicatietechnieken is de fysieke locatie van de servicedesk niet meer relevant. Door wereldwijd verschillende lokale servicedesks te beschouwen als een virtuele servicedesk, kan 24 uur support worden geleverd.
9. Skilled: de medewerker van de servicedesk bezit enige kennis en deskundigheid en zal eenvoudige problemen proberen op te lossen aan de hand van gedocumenteerde oplossingen. Unskilled: bij deze vorm van servicedesk worden de binnenkomende calls

geregistreerd, globaal vastgelegd en meteen doorgestuurd naar gespecialiseerde afdelingen. Er wordt vooral gewerkt met standaardprocedures en scripts voor de afhandeling.

10. Rapportages voor de klant: of de telefoon snel genoeg wordt opgenomen, of de gebruikers vriendelijk en correct te woord worden gestaan en of de gebruiker de juiste adviezen krijgt. Ook wordt gemeten of storingen op tijd worden opgelost, en of de gebruikers tijdig worden gewaarschuwd voor aankomende problemen. Rapportages voor het management: het aantal opgeloste problemen belangrijk, het aantal calls per werkplek, de gemiddelde tijd per call en of er gebruikers zijn die buiten de servicedesk om contact proberen te leggen met de specialisten van de IT-afdeling.

**Waar/niet waar:**

1. Niet waar
2. Waar
3. Niet waar
4. Waar
5. Niet waar
6. Waar
7. Waar
8. Waar
9. Niet waar
10. Waar

**Meerkeuzeopgaven:**

1. B
2. B
3. B
4. A
5. D
6. B
7. C
8. B
9. D
10. A

## Hoofdstuk 6 Configuration management

### Vragen en opdrachten met betrekking tot de casus:

1. BIS, PC, laptop, softwarelicenties, cursusmap.
2. BIS: versie, naam, datum laatste wijziging.  
PC: type, merk, serienummer, type processor, datum van aanschaf, grootte harddisk.  
Laptop: type, merk, serienummer, type processor, datum van aanschaf, grootte harddisk.  
Softwarelicentie: naam, type, aankoopbedrag, versie, serienummer, leverancier  
Cursusmap: naam, type, soort, datum, opbergplaats, eigenaar.
3. Beleid ontwikkelen, opzetten CMDB, identificeren van de CI's, beheer CMDB, bewaken van de status van de CI's, uitvoeren van audits, rapporteren.
4. PC's en laptops zijn verbonden met een centrale server, een pc is verbonden met een printer, een module is onderdeel van een programma (bijvoorbeeld BIS), een monitor is onderdeel van een PC.
5. Een PC met MS-Office, BIS, internet-toegang en e-mail.
6. Verificatie: iedere keer als een storing wordt gemeld worden de relevante attributen van het betrokken CI gecontroleerd. Audits: controle, eventueel in de vorm van een steekproef om te controleren of de gegevens uit de CMDB nog overeenkomen met de werkelijk situatie, bijvoorbeeld het aantal PC's en laptops, waar ze zich bevinden enz.
7. Een overzicht voor het management met alle relevante onderdelen van de IT-infrastructuur, snelle afhandeling van storingen door verbeterde registratie, publiceren van een lijst met veelvoorkomende vragen, problemen en oplossingen.
8. Beantwoorden van vragen van gebruikers, geven van advies, telefonisch oplossen van storingen, registreren van storingen en doorverwijzen van storingen naar de juiste persoon. Op de hoogte houden van de gebruikers over de voortgang van gemelde storingen.
9. Alle IT-middelen worden geregistreerd en kunnen voortaan worden beheerst en bewaakt. Doordat minder snel dingen zoek raken kunnen kosten worden bespaard, wijzigen in de IT-infrastructuur kunnen sneller worden doorgevoerd doordat snel inzicht kan worden verkregen in de betrokken CI's. Verbeterde registratie van storingen en problemen, sneller oplossen van problemen en storingen en minder kans op het gebruik van illegale kopieën, doordat deze worden ontdekt, kortom een stabielere IT-infrastructuur.
10. Stabielere werkomgeving, beter inzicht in de kosten, beter kunnen overzien van de consequenties van wijzigingen in de IT-infrastructuur, klanten en medewerkers zijn meer tevreden over de IT-infrastructuur.
11. Medewerkers kunnen de nieuwe manier van werken als bureaucratisch ervaren, er gaat veel energie zitten aan het onderhouden van de CI's, gebrek aan afstemming met andere beheerprocessen als wijzigingsbeheer, waardoor de CMDB niet meer actueel is, bij urgente wijzigingen is er altijd het gevaar dat de CMDB niet wordt bijgewerkt, te ambitieuze planning en gebrek aan acceptatie bij management en medewerkers.



**Open vragen:**

1. De registratie van en het verschaffen van informatie over alle relevante onderdelen van de IT-infrastructuur.
2. CI: Configuratie Item: ieder voor het beheer relevant onderdelen van de IT-infrastructuur. CMDB: Configuration Management DataBase, de database met CI's, waarin onder andere ook de relaties tussen de CI's kunnen worden vastgelegd.
3. Asset management: registreren van vooral financiële gegevens van hard- en software, bijvoorbeeld de aanschafwaarde, afschrijving en locatie. Configuration management gaat veel verder: de CI's worden niet alleen geregistreerd, maar ook wordt de status bewaakt, worden de relaties tussen de CI's in kaart gebracht en worden wijzigingen geregistreerd.
4. Planning, identificatie, controle, statusbewaking, verificatie en rapportage.
5. Beheren van het datamodel van de CMDB, informatievoorziening aan de andere beheerprocessen, maken van rapportages en planning van de activiteiten die betrekking hebben op het proces.
6. Bereik: bepalen welke onderdelen van de IT-infrastructuur onder controle moeten worden gebracht van Configuration Management.
7. Diepgang: de diepte van de registratie, bijvoorbeeld of van een softwaresuite alleen de suite zelf moet worden geregistreerd, of moeten ook de individuele programma's en de modules worden geregistreerd?
8. Fysiek: dingen die fysiek bij elkaar horen, bijvoorbeeld een bepaalde module is onderdeel van een bepaald programma. Logisch: dingen die logisch gezien bij elkaar horen, een bepaalde procedure heeft bijvoorbeeld betrekking op een bepaald programma.
9. De kenmerken van de CI's. Het configuratie item PC heeft bijvoorbeeld als attributen een serienummer, kleur, leverancier, leverdatum etc.
10. Unieke identificatie, simpele en makkelijk te onthouden nummering.
11. Een baseline is een kopie van een groep bevroren CI's die zijn getest en daarna niet meer zijn aangepast.
12. In gebruik, in reparatie, in ontwikkeling.
13. Verificatie: iedere keer als een storing wordt gemeld, wordt gecontroleerd of de gegevens van het betrokken CI nog kloppen. Audit: periodieke controle van de gegevens van alle CI's uit de CMDB.
14. Muteren en verifiëren van de CI's uit de CMDB.
15. Het goed uitvoeren van dit proces verlaagt de kosten van het beheren van de IT-infrastructuur en verhoogt de kwaliteit van de aangeboden diensten.
16. Medewerkers kunnen de nieuwe manier van werken als bureaucratisch ervaren, er gaat veel energie zitten aan het onderhouden van de CI's, gebrek aan afstemming met andere beheerprocessen als wijzigingsbeheer, waardoor de CMDB niet meer actueel is, bij urgente wijzigingen is er altijd het gevaar dat de CMDB niet wordt bijgewerkt, te ambitieuze planning en gebrek aan acceptatie bij management en medewerkers.
17. Configuration Management heeft relaties met alle andere processen van de Service Support Set en van de Service Delivery Set: alle incidenten, problemen en wijzigingen hebben betrekking op de CI's uit de CMDB.

**Waar/niet waar:**

1. Niet waar
2. Waar
3. Waar
4. Waar
5. Niet waar
6. Waar
7. Waar
8. Waar
9. Niet waar
10. Niet waar
11. Waar
12. Waar
13. Waar
14. Waar

**Meerkeuzeopgaven:**

1. B
2. C
3. D
4. D
5. A
6. B
7. C
8. D

## Hoofdstuk 7 Incident Management

### Vragen en opdrachten met betrekking tot de casus:

1. Detectie, aanneming, registratie, classificatie, analyse, diagnose, oplossing, herstel, bewaking.
2. Datum, tijd, betrokken CI, korte omschrijving incident, naam gebruiker, status, prioriteit.
3. De werkdruk is bij alle IT-medewerkers flink afgenomen.
4. Urgentie: een probleem met BIS moet meteen worden opgelost, anders worden de primaire bedrijfsprocessen verstoord. Impact: de gevolgen van een probleem met BIS kan grote gevolgen hebben voor de primaire bedrijfsprocessen, die erdoor verstoord worden.
5. Ja, alle incidenten komen binnen op de servicedesk, waar ze door Jeroen en Monique worden geregistreerd. Als de deze een probleem niet op kunnen lossen, worden de problemen in eerste instantie doorgestuurd naar Abdel en Jerrol. Als die er ook niet uitkomen sturen ze de problemen door naar Jaap of José.
6. Hier is sprake van functionele escalatie, omdat het probleem wordt doorgestuurd naar iemand met meer kennis.
7. Eerste lijn: Jeroen en Monique, tweede lijn: Abdel en Jerrol, derde lijn: Jaap en José.
8. Ben, hij belt buiten de servicedesk om met Jaap.
9. In eerste instantie via voorlichting en bewustwording: uitleggen waarom alle incidenten via de servicedesk moeten worden gemeld.
10. Alle incidenten worden gekoppeld aan de CI's uit de CMDB, hierdoor worden de CI's voortdurend geverifieerd.

### Open vragen:

1. Een incident is een gebeurtenis die afwijkt van de standaardwerking van een IT-dienst en die de kwaliteit van die dienst vermindert of verstoort. Een service request is een verzoek van de gebruiker om informatie, advies of ondersteuning.
2. Incidenten: gebruiker kan niet inloggen op het netwerk, gebruiker kan niet printen, applicatie “hangt”, gebruiker kan geen verbinding krijgen met internet, gebruiker kan geen e-mail versturen, systeemmeldingen als “harde schijf raakt vol”.  
Service Requests: gebruiker is zijn wachtwoord vergeten, een verzoek om informatie; advies bij gebruik van een applicatie; onduidelijkheid in de gebruikersdocumentatie.
3. Een tijdelijke herstelactie, bijvoorbeeld het plaatsen van een reserveprinter, zodat de gebruiker snel verder kan werken.
4. Detectie, aanneming en registratie, classificatie, matchen, analyse en diagnose, oplossen en herstel, afsluiten, voortgang bewaken.
5. De servicedesk medewerker controleert of een vergelijkbaar incident eerder is voorgekomen en of er een oplossing of een work-around beschikbaar is.
6. Door de servicedesk medewerker doorverwijzen van incidenten waarvoor geen oplossing is of waarvoor meer expertise nodig is naar iemand met meer kennis of met meer beslissingsbevoegdheid.
7. Functioneel: iemand sturen met meer kennis (ook wel horizontale escalatie).  
Hiërarchisch: iemand sturen met meer bevoegdheden (ook wel verticale escalatie).
8. De servicedesk is de eerstelijnsupport, incidenten die ze niet kunnen oplossen worden doorverwezen naar de tweedelijnsupport: specialistische teams, als die er ook niet uit komen kunnen de incidenten nog worden doorverwezen naar de derdelijnsupport: de ontwikkelaars of de vierdelijnsupport: de leveranciers.
9. Toename van de stabiliteit en continuïteit van de IT-dienstverlening, minder verstoring van de bedrijfsprocessen, verbeterde productiviteit van de gebruikers, grotere

tevredenheid van de gebruikers, lagere kosten, op de juiste wijze inzetten van de beschikbare IT-mensen, zinvolle managementrapportage.

10. Omzeilen van de procedures, geen duidelijk verschil tussen incidenten en problemen, geen duidelijke afspraken met de klant over het niveau van de dienstverlening, cultuurverandering stuit op weerstanden, onvoldoende kennis over de business bij de medewerkers van de service desk, gebrek aan kennis en ervaring bij de medewerkers van de service desk.
11. Alle incidenten komen binnen op de servicedesk, waar de incidenten worden gekoppeld aan de CI's uit de CMDB. Vervolgens zorgt Incident Management ervoor dat de incidenten worden geanalyseerd en indien mogelijk verholpen.

**Waar/niet waar:**

1. Niet waar
2. Waar
3. Niet waar
4. Waar
5. Niet waar
6. Waar
7. Niet waar
8. Waar
9. Niet waar
10. Waar

**Meerkeuzeopgaven:**

1. A
2. D
3. D
4. D
5. A
6. C
7. D
8. B
9. D
10. D
11. B
12. A
13. A

## Hoofdstuk 8 Problem Management

### Vragen en opdrachten met betrekking tot de casus:

1. Jeroen, Monique, Jaap, José, Hans, Abdel, Jerrol.
2. Incident: storing in BIS, problem: incident met onbekende oorzaak dat niet meteen door Jeroen en Monique kan worden opgelost, known error: probleem met de datacommunicatieverbinding als er vanuit meer dan twee vestigingen tegelijkertijd wordt ingebeld, work-around: rooster waarin de medewerkers van de vestigingen op welke tijden ze kunnen inbellen, change: uitbreiden van de capaciteit van de datacommunicatieverbindingen.
3. Jeroen en Monique.
4. Tweede lijn: Abdel en Jerrol, Derde lijn: Hans en José, Vierde lijn: Jaap en leveranciers.
5. Een database opbouwen met known errors, zodat deze er al bij de service desk kunnen worden uitgefilterd.
6. Hans en José.
7. Storingen in het netwerk en in BIS worden in eerste instantie opgelost door incident management. Als de medewerkers van incident management een incident niet kunnen oplossen, wordt het incident doorspeeld naar problem management, waar het probleem wordt geanalyseerd en vergeleken met andere incidenten. De incidentenregistratie is een belangrijk hulpmiddel voor problem management.
8. Het aantal incidenten neemt drastisch af en de stabiliteit van de IT-infrastructuur neemt toe. Als gevolg hiervan neemt de tevredenheid bij de gebruikers toe en de werkdruk bij de IT-afdeling af.
9. Gebrek aan betrokkenheid bij de specialisten, te weinig overdracht van known errors door de ontwikkelafdeling, beperkte koppeling tussen incident management en problem management.
10. Configuration Management levert alle relevante informatie over de IT-infrastructuur aan problem management. Problem Management gaat bij de analyse van een probleem altijd op zoek naar de betrokken CI's. Incident Management is de belangrijkste leverancier voor Problem Management. De gegevens uit de incidentenregistratie worden gebruikt bij het opsporen van problemen. Andersom levert Problem Management known errors, work-arounds en quick fixes waarmee het optreden van incidenten wordt geminimaliseerd.

### Open vragen:

1. Het analyseren van incidenten om op die manier fouten in de IT-infrastructuur op te sporen en op te lossen.
2. Reactief problem management reageert pas als er een probleem is gemeld, proactief problem management probeert problemen te voorkomen.
3. Een incident is een gebeurtenis die de kwaliteit van een dienst vermindert of verstoort. Incidenten kunnen ons op het spoor brengen van een probleem: een fout in de IT-infrastructuur met een onbekende oorzaak. Een known error is een probleem met een bekende oorzaak. Door registratie van de known errors krijgen de medewerkers van de servicedesk meer inzicht en kunnen ze meer storingen telefonisch oplossen. Problem management en incident management kunnen gebruik van een work-around (alternatieve manier van werken) of een quick fix (snelle voorlopige wijziging), zodat de gebruiker verder kan werken.
4. De servicedesk is de eerstelijnsupport, incidenten die ze niet kunnen oplossen worden doorverwezen naar de tweedelijnsupport: specialistische teams, als die er ook niet uit komen kunnen de incidenten nog worden doorverwezen naar de derdelijnsupport: de ontwikkelaars of de vierdelijnsupport: de leveranciers.

5. Daarmee wordt bedoeld dat van een probleem de oorzaak nog niet bekend is, dit in tegenstelling tot de known error.
6. Problem Control: het onderzoeken van problemen. Error Control: het bewaken van known errors. Proactief beheer: het voorkomen van problemen. Trendanalyse: het vroegtijdig opsporen van mogelijke fouten. Rapportage: het verschaffen van informatie.
7. Identificatie en registratie, classificatie en allocatie en onderzoek en diagnose.
8. Identificatie en registratie, onderzoek, noodoplossing doorvoeren, vastleggen oplossing, post implementation review, volgen en bewaken en informatie verschaffen.
9. Elke wijziging moet worden geëvalueerd. Daarvoor wordt een Post Implementation Review (PIR) uitgevoerd. Is de wijziging succesvol, dan kan het probleem worden afgesloten. Daarnaast vindt communicatie plaats naar Incident Management zodat ook de bijbehorende incidenten kunnen worden gesloten.
10. Het goed uitvoeren van het proces probleembeheer kan de IT-afdeling een belangrijke kwaliteitsimpuls geven doordat het aantal incidenten drastisch afneemt en de stabiliteit van de IT-infrastructuur toeneemt. Als gevolg hiervan neemt de tevredenheid bij de gebruikers toe en de werkdruk bij de IT-afdeling af.
11. Gebrek aan betrokkenheid bij de specialisten, te weinig overdracht van known errors door de ontwikkelafdeling, beperkte koppeling tussen incident management en problem management.
12. Alle Service Support-processen hebben een nauwe band met Problem Management: Configuration Management levert alle relevante informatie over de IT-infrastructuur, de gegevens uit de incidentenregistratie van Incident Management worden gebruikt bij het opsporen van problemen, ook Availability Management en Capacity Management zijn belangrijke leveranciers van informatie over mogelijke problems.
13. Als het proces Problem Management goed functioneert, worden er veel known errors geregistreerd, waardoor de servicedesk meer mogelijkheden heeft om incidenten snel op te lossen.

**Waar/niet waar:**

1. Niet waar
2. Waar
3. Waar
4. Waar
5. Waar
6. Waar
7. Waar
8. Waar
9. Niet waar
10. Waar

**Meerkeuzeopgaven:**

1. A
2. A
3. A
4. D
5. B
6. C
7. A
8. B
9. B
10. C

## Hoofdstuk 9 Change Management

### Vragen en opdrachten met betrekking tot de casus:

1. Omwisselen van een muis of een printer, installatie van een printer- of muisdriver.
2. Wijzigingsverzoeken worden ingediend bij de servicedesk en worden in eerste instantie door José beoordeeld. Indien nodig roept zij de wijzigingsadviescommissie bijeen, die een vergadering belegt waar alle betrokken aanwezig zijn.
3. Beoordelen van de wijzigingen.
4. Registratie, acceptatie, classificatie, planning, coördinatie en evaluatie.
5. José en Jaap, aangevuld met wisselende vertegenwoordigers van gebruikers, beheerders en ontwikkelaars, afhankelijk van de aard van de wijziging.
6. Afhankelijk van het aantal wijzigingsverzoeken waarschijnlijk enkele keren per jaar.
7. Ja, de niet urgente wijzigingen kunnen worden gecombineerd en kunnen bij een volgende release worden doorgevoerd.
8. José en Jaap, aangevuld met gebruikers, ontwikkelaars en beheerders.
9. Bij de urgente wijzigingsprocedure moeten zoveel mogelijk de stappen van de normale wijzigingsprocedure worden doorlopen. Om tijd te winnen kan de autorisatie worden versneld, kan de testprocedure worden verkort en kan de administratie achteraf worden bijgewerkt. Deze stappen komen overeen met de urgente wijzigingsprocedure bij Bikefun.
10. Soort, datum, gerelateerd probleem, betrokken CI's, reden, aanvrager, omschrijving wijziging.

### Open vragen:

1. Het analyseren, autoriseren en coördineren van wijzigingen, zodat aan wijzigingen gerelateerde incidenten zoveel mogelijk worden voorkomen.
2. Om een wijziging te kunnen doorvoeren moet een Request for Change (RfC), een wijzigingsverzoek, een verzoek om aanpassing van de IT-infrastructuur worden ingediend. Voor zwaardere changes wordt de hulp ingeroepen van de Change Advisory Board (CAB), een overlegorgaan dat op gezette tijden bijeenkomt om changes te beoordelen en te plannen in een Forward Schedule of Changes (FSC), de planning van alle geautoriseerde changes.
3. Problem Management, de klant, het management, Service Level Management, Availability Management, Capacity Management, de overheid, leveranciers, project management, de medewerkers van de IT-afdeling.
4. Registratie, acceptatie, classificatie, planning, coördinatie, evaluatie.
5. Prioriteit: laag, middel, hoog of urgent, afhankelijk van de overlast en de betrokken gebruikers. Categorie: lage, significante en grote impact, afhankelijk van de impact op de bedrijfsprocessen en de benodigde resources.
6. Ongeautoriseerde changes, wijzigingsverzoeken (rfc's), lopende en afgehandelde changes, evaluaties van de uitgevoerde changes.
7. Versneld autoriseren, testprocedure verkorten en de administratie achteraf bijwerken.
8. De laatste goedwerkende versie voordat de change werd doorgevoerd.
9. Als de change mislukt.
10. Probleemoriëntatie informatievoorziening, onderzoeken organisatieaspecten, analyseren veranderingsvermogen, vaststellen gewenste situatie informatievoorziening, opstellen projectplan, inrichten projectorganisatie, samenstellen release, uitvoeren gegevensconversie, verzorgen van kennisoverdracht, opstellen wijzigingsvoorstel, bewaken systeemonderhoud, bepalen migratiestap, bepalen conversiestrategie, goedkeuren/beoordelen opdracht, verzoek, e.d., afbakenen onderzoeksgebied, opstellen

- normen, criteria, randvoorwaarden, opstellen kwaliteitsplan, uitvoeren analyse, uitvoeren risicoanalyse, aansturen, coördineren activiteit.
11. Dat is afhankelijk van het aantal wijzigingsverzoeken, gemiddeld 1 keer per maand. Onderwerpen die worden besproken: ongeautoriseerde changes, wijzigingsverzoeken (rfc's), lopende en afgehandelde changes, evaluaties van uitgevoerde changes.
  12. Aantallen changes in een bepaalde periode, gerubriceerd per CI, oorzaken van changes, aantal geslaagde en mislukte changes, aantal fall-backsituaties, aantallen incidenten in relatie tot changes, de snelheid waarmee de wijzigingen worden doorgevoerd, aantallen incidenten ten gevolge van changes, kosten van de uitgevoerde changes, trendanalyses en grafieken van changes over de verschillende periodes.
  13. Het registreren van changes en de impactanalyse van changes vindt plaats onder de controle van Configuration Management. Van de andere kant leidt een change altijd tot een wijziging in de status van het betrokken CI, dat vervolgens onder verantwoordelijkheid van Configuration Management moet worden gewijzigd.
  14. Changes worden vaak door Problem Management aangevraagd als oplossing voor een probleem. Na het uitvoeren van een change moet worden gecontroleerd of het achterliggende probleem is opgelost.
  15. Standaardchanges zijn omschreven en goedgekeurde changes als het verwisselen van de muis of het installeren van een stuurprogramma. Deze wijzigingen kunnen routinematig worden uitgevoerd, er hoeft geen wijzigingsverzoek voor te worden ingediend.
  16. Door regelmatig audits uit te voeren en controles uit te voeren op changes, CI's, en incidenten.
  17. Ja, ze maken onderdeel uit van de change-procedure en mogen geen ongeautoriseerde changes doorvoeren.

**Waar/niet waar:**

1. Niet waar
2. Niet waar
3. Waar
4. Niet waar
5. Niet waar
6. Waar
7. Waar
8. Niet waar
9. Waar
10. Waar
11. Waar
12. Waar

**Meerkeuzeopgaven:**

1. B
2. B
3. A
4. B
5. B
6. A
7. D
8. A
9. A
10. C



## Hoofdstuk 10 Release Management

### Vragen en opdrachten met betrekking tot de casus:

1. Distributie en implementatie van nieuwe versies van BIS, wijzigingsvoorstellen van leveranciers, gebruiken van verschillende versies op de vestigingen, terugdraaien van een mislukte invoering van een nieuwe release, doorvoeren van wijzigingen in twee verschillende versies.
2. Gebruikers, IT-medewerkers, leveranciers.
3. Er zullen minder incidenten optreden als gevolg van de implementatie van een nieuwe versie van BIS, de gebruikers worden beter op de hoogte gesteld van de planning van de uitrol van nieuwe versies van apparatuur en programmatuur, er is minder kans op illegale kopieën en deze worden eerder ontdekt, de organisatie in staat is de software- en hardware versies over meerdere locaties te standaardiseren, zodat het beheer ervan gemakkelijker wordt, de software die wordt gebruikt van goede kwaliteit is doordat deze uitgebreid is getest, incidenten ten gevolge van versieconflicten worden voorkomen.
4. Automatisch, via het netwerk.
5. Ontwerp, broncode, doelcode, geaccepteerde versie.
6. Toetsenborden, muizen, hard disks, CD-spelers, diskteststations, monitoren.
7. Welke acties moeten worden ondernomen om de service te herstellen als een uitrol van een nieuwe release geheel of gedeeltelijk faalt.
8. Weerstand bij de medewerkers, omzeilen van de procedures, urgente wijzigingen worden buiten release management om uitgevoerd, er kunnen versieverschillen ontstaan tussen de verschillende locaties, niet goed testen omdat de inrichting van een representatieve testomgeving te kostbaar is.
9. Onder andere configuration management, change management en service level management.
10. Aanspreekpunt naar de gebruiker met betrekking tot de distributie van nieuwe releases.

**Open vragen:**

1. Het beheren en distribueren van alle hardware- en softwareversies die in gebruik zijn en door de IT-afdeling worden ondersteund.
2. Er treden minder incidenten op als gevolg van de implementatie van een nieuwe versie, de gebruikers zijn beter op de hoogte van de planning van de uitrol van nieuwe versies van apparatuur en programmatuur, er is minder kans op illegale kopieën en deze worden eerder ontdekt, de organisatie is in staat de software- en hardware versies over meerdere locaties te standaardiseren, zodat het beheer ervan gemakkelijker wordt, de software die wordt gebruikt is van goede kwaliteit doordat deze uitgebreid is getest, incidenten ten gevolge van versieconflicten kunnen worden voorkomen.
3. Een release of uitgave bestaat uit het geheel van nieuwe, gewijzigde en bestaande CI's dat op een moment beschikbaar wordt gesteld voor exploitatie. CI's binnen een release kunnen bestaan uit programmatuur, apparatuur, documentatie en procedures.
4. Een major release is een belangrijke uitrol van gewijzigde CI's, met meestal een aanzienlijke uitbreiding van de functionaliteit. Deze releases bieden vaak oplossingen voor een aantal known errors, work-arounds en quick fixes. Deze releases worden vaak geïdentificeerd als versie 1, versie 2, etc. Een minor release is een uitrol van slechts een beperkt aantal gewijzigde CI's, met kleine wijzigingen in de functionaliteit en kleine verbeteringen voor known errors, work-arounds en quick fixes. Deze releases worden vaak geïdentificeerd als versie 2.1, versie 2.2, etc.
5. Een set spoedeisende wijzigingen, die niet kunnen worden uitgesteld en die een tijdelijke oplossing bieden voor een problem of een known error. Deze releases worden vaak geïdentificeerd als versie 2.1.1, 2.1.2, etc.
6. Delta-, full- en package release.
7. De Definitive Software Library (DSL) is een beschermde omgeving waar alle geautoriseerde versies van software-CI's worden opgeslagen en beschermd. Deze beschermde omgeving kan bestaan uit verschillende softwarebibliotheken die gescheiden worden van de ontwikkel-, de test- en de exploitatieomgeving. De DSL bevat een kopie van alle aangeschafte en ontwikkelde software inclusief licentiegegevens en documentatie. Nieuwe releases worden ontwikkeld en samengesteld op basis van de software-items uit de DSL.
8. De Definitive Hardware Store (DHL) is de opslagplaats voor alle reserveonderdelen en hardwarevoorraden. Ook dit is een beschermde omgeving, waarvan alle items worden geregistreerd als CI's in de CMDB. Als de CI's worden gebruikt om tijdelijk een defect CI uit de exploitatieomgeving te vervangen, moeten het betreffende CI na afloop weer worden teruggezet in de DHL.
9. Bij elke nieuwe release moet er een back-outplan worden opgesteld waarin staat omschreven welke acties moeten worden ondernomen om de service te herstellen als een uitrol van een nieuwe release geheel of gedeeltelijk faalt.
10. Releasebeleid en –planning, ontwerpen, bouwen en samenstellen van de release, testen en acceptatie van de release, uitrolplanning, communicatie, voorbereiding en training, release-distributie en installatie.
11. Big Bang: de release wordt in een keer in zijn geheel uitgerold. Gefaseerd: de release wordt in verschillende fasen uitgerold, dit kan alleen als de oude en de nieuwe versie geen aanleiding geven tot versieconflicten. Incrementeel: naar functionaliteit: alle gebruikers krijgen tegelijkertijd een stukje nieuwe functionaliteit erbij. Incrementeel: naar locatie: alle gebruikers van een bepaalde locatie worden in een keer uitgerold. Evolutionair: de functionaliteit wordt in de loop van de tijd geleidelijk in fasen uitgerold.
12. Release Management rapporteert regelmatig aan het management over de op handen zijnde releaseplannen, de afgehandelde releases, de testresultaten, de problemen bij

planning en distributie, de mate waarin de releases op tijd konden worden afgerond, het aantal keren dat een release tot een back-out leidde en het aantal aangetroffen ongeautoriseerde versies.

13. Weerstand bij de medewerkers, omzeilen van de procedures, urgente wijzigingen worden buiten release management om uitgevoerd, er kunnen versieverschillen ontstaan tussen de verschillende locaties, niet goed testen omdat de inrichting van een representatieve testomgeving te kostbaar is.

**Waar/niet waar:**

1. Niet waar
2. Niet waar, juist andersom
3. Waar
4. Waar
5. Waar
6. Niet waar
7. Waar
8. Waar
9. Niet waar
10. Niet waar

**Meerkeuzeopgaven:**

1. B
2. A
3. D
4. D
5. B
6. A
7. B
8. B
9. C
10. A

## Hoofdstuk 11 Service Level Management

### Vragen en opdrachten met betrekking tot de casus:

1. Voor de IT-afdeling is Ben degene die bij Bikefun afspraken maakt namens de gebruikers en dus de klant. Leveranciers zijn: Telcom voor de datacommunicatielijnen, I-net voor internet en e-mail verkeer en Qcom voor de levering van hardware en software.
2. Werktijden, met name 's-avonds en in het weekend, snel oplossen van problemen, snelle vervanging van defecte onderdelen.
3. Openingstijden van de servicedesk, leveringstijden van leveranciers, beschikbaarheid van IT-diensten als datacommunicatielijnen, internet en e-mail, afspraken met interne IT-afdelingen.
4. Openingstijden van de servicedesk, oplostijden van incidenten en problemen, beschikbaarheid van e-mail, internet en BIS, wijzigingsprocedures.
5. Ja, bijvoorbeeld over het oplossen van problemen in BIS.
6. Ja, bijvoorbeeld over de beschikbaarheid van datacommunicatieverbindingen, internet en e-mail en het leveren van onderdelen die vervangen moeten worden.
7. Openingstijden van de servicedesk, oplostijden van storingen, wijzigingsprocedures, beschikbaarheid van IT-diensten als BIS, internet en e-mail.
8. Bereikbaarheid van de servicedesk, oplospercentage van storingen, gemiddelde duur van storingen, klantvriendelijkheid van de medewerkers van de servicedesk.
9. Grotere tevredenheid bij de klant, verbeterde zakelijke prestatie van de IT-afdeling, betere kwaliteit van de dienstverlening, de klant kan een goede afweging maken tussen kwaliteit en kosten, kostenbesparingen door toegenomen kostenbewustzijn.
10. De klant heeft soms veel moeite om precies te formuleren wat de eisen en verwachtingen van een dienst zijn. Het kost veel moeite om elke dienst uit te drukken in meetbare waarden. Er moet worden opgepast voor te ambitieuze plannen, die niet kunnen worden waargemaakt. Er is veel overhead nodig om de service levels te meten en bewaken. Vaak wordt begonnen met het opstellen van SLA's, die geen inhoud hebben doordat de stappen van het proces Service Level Management niet worden gevolgd.

### Open vragen:

1. Geredeneerd vanuit SLM is een gebruiker iemand die gebruik maakt van IT-diensten. De klant is degene die namens een organisatie bevoegd is om afspraken te maken over de afname van IT-diensten.
2. Leveranciers van IT-diensten zijn nodig om de aan de afspraken met de klant te voldoen.
3. De behoeften van de klant. Service Level Requirements (SLR) worden gebruikt voor het opzetten, aanpassen en vernieuwen van diensten.
4. De Service Specsheets is een vertaling van de externe behoeften van de klant naar de interne specificaties om de dienst te kunnen verwezenlijken. In de Service Specsheets wordt ook een koppeling gelegd tussen de diensten en de interne en externe leveranciers die nodig zijn om de dienst in stand te kunnen houden. De Specsheets zijn technische documenten, bestemd voor de IT-medewerkers
5. Een gedetailleerd overzicht van de aangeboden diensten en het niveau van de dienstverlening. De Service Catalogue is een belangrijk communicatiemiddel voor de klant. De Service Catalogue is bedoeld voor de klant en moet de diensten in voor de klant begrijpelijke bewoordingen beschrijven.
6. Een SLA is een overeenkomst tussen de IT-organisatie en de klant, waarin de afgesproken diensten worden omschreven in niet-technische termen. Het SLA heeft een beperkte looptijd en geeft de norm aan voor het meten en sturen van de IT-diensten. Sommige afspraken in een SLA zijn algemeen en gelden voor de gehele organisatie, andere

afspraken zijn meer specifiek en worden lager in de organisatie overeengekomen.

Onderwerpen die in een SLA worden besproken zijn: de openingstijden van de servicedesk, de oplostijden van storingen, wijzigingsprocedures, de beschikbaarheid van IT-diensten en de IT-diensten die worden aangeboden.

7. Interne dienstverleners: OLA, externe leveranciers: onderpinning contracts.
8. Service Level Management (dienstniveaubeheer) is verantwoordelijk voor het continu onderhouden en verbeteren van de met de klant overeengekomen dienstverlening door met de klant te onderhandelen over de aangeboden diensten, afspraken te maken over deze diensten en vervolgens de afgesproken diensten te monitoren en erover te rapporteren aan de klant.
9. Afspraken maken: identificeren, definiëren en contracteren.  
Afspraken borgen: monitoren, rapporteren en evalueren.
10. De interne normen zijn technisch van aard en zijn bedoeld voor de medewerkers van de IT-afdeling, de externe normen zijn bedoeld voor de klant en moeten in voor de klant begrijpelijke taal worden opgesteld.
11. Grotere tevredenheid bij de klant, verbeterde zakelijke prestatie van de IT-afdeling, betere kwaliteit van de dienstverlening, de klant kan een goede afweging maken tussen kwaliteit en kosten, kostenbesparingen door toegenomen kostenbewustzijn.
12. De klant heeft soms veel moeite om precies te formuleren wat de eisen en verwachtingen van een dienst zijn. Het kost veel moeite om elke dienst uit te drukken in meetbare waarden. Er moet worden opgepast voor te ambitieuze plannen, die niet kunnen worden waargemaakt. Er is veel overhead nodig om de service levels te meten en bewaken. Vaak wordt begonnen met het opstellen van SLA's, die geen inhoud hebben doordat de stappen van het proces Service Level Management niet worden gevolgd.

**Waar/niet waar:**

1. Niet waar
2. Waar
3. Waar, zie bladzijde 167 onderaan
4. Niet waar
5. Waar
6. Niet waar
7. Waar
8. Niet waar, identificeren is de eerste stap, zie de tekening op blz. 166
9. Waar, een service specsheet is een vertaling van de behoeften van de klant naar de interne specificaties om de dienst te kunnen verwezenlijken.
10. Waar

**Meerkeuzeopgaven:**

1. B
2. C
3. A
4. C
5. B
6. B, de Service Catalogue is bestemd voor de klant, de andere documenten zijn bestemd voor de medewerkers van de IT-afdeling, dus intern.
7. D, het SLA is bedoeld voor de klant, er staan dus geen technische specificaties in.
8. C, het resultaat van een review (evaluatie) is een verbeterprogramma (SIP).
9. B
10. B

## Hoofdstuk 12 Financial Management for IT-Services

### Vragen en opdrachten met betrekking tot de casus:

1. Inzicht krijgen in de kosten van IT-diensten.
2. Budgeting, accounting en charging.
3. Directe kosten: kosten van printen, e-mailen, gebruik van BIS, gebruik van internet, gebruik van MS-Office. Indirecte kosten: kosten van de werkplek en de kosten van de administratie en de boekhouding.
4. Vaste kosten: hardware, software, IT-medewerkers, gebouwen. Variabele kosten: kosten van papier, toner, internetgebruik, e-mailgebruik.
5. Capitalkosten: afschrijvingen op hardware en software. Revenuekosten: verzekeringen, onderhoudscontracten en licenties.
6. Hardwarekosten: de kosten van de gebruikte apparatuur als computers en printers. Softwarekosten: de kosten van de gebruikte software als BIS en MS-Office. Personeelskosten: de kosten van het IT-personeel. Huisvestingskosten: de kosten van kantoorruimte van het hoofdkantoor en de verschillende vestigingen. Uitbestedingskosten: de kosten van de uitbestede IT-diensten. Overdraagbare kosten: kosten die de interne afdelingen bij elkaar in rekening brengen.
7. Voorlopig ligt incremental budgeting het meest voor de hand, aangezien de cijfers voor verleden jaar een goede basis vormt voor het budget voor volgend jaar. In een later stadium kan worden overgeschakeld op zero-based budgeting.
8. Target return ligt het meest voor de hand, omdat er nergens over wordt gesproken dat de IT-afdeling winst moet gaan maken.
9. Er kan een keuze worden gemaakt tussen accounting center en recovery center.
10. Grotere tevredenheid bij de klant, verbeterde zakelijke prestatie van de IT-afdeling, betere kwaliteit van de dienstverlening, de klant kan een goede afweging maken tussen kwaliteit en kosten, kostenbesparingen door toegenomen kostenbewustzijn.

**Open vragen:**

1. Te voorzien in een kosteneffectief beheer van de IT-middelen door de kosten te identificeren en vervolgens te relateren aan de geleverde IT-diensten.
2. Klantwensen, kwaliteit en kosten.
3. De klant wil vaak veel, van een hoge kwaliteit en tegen lage kosten.
4. De financiële cyclus bestaat uit de drie hoofdactiviteiten budgeting, accounting en charging:
5. Directe kosten: deze kosten zijn verbonden met de levering van een IT-product of -dienst en kunnen direct en specifiek aan dit product of deze dienst worden toegerekend, bijvoorbeeld de telefoonkosten van een internetverbinding. Indirecte kosten: overhead, kosten die zijn verbonden met de levering van een IT-product of -dienst, die niet direct en specifiek aan dat product of die dienst kunnen worden toegerekend, bijvoorbeeld de kosten van de werkplek of de kosten van ondersteunende diensten als administratie.
6. Hoofdelijk omslaan en activity based costing.
7. Vaste kosten: dit zijn de kosten die zijn verbonden met de levering van een IT-product of dienst die niet afhankelijk zijn van de hoogte van de productie. Investerings in hardware, software, vaste medewerkers en gebouwen zijn voorbeelden van vaste kosten. Van de vaste kosten worden meestal niet de aanloopkosten opgevoerd, maar de periodieke afschrijvingen. Bij een computer bijvoorbeeld die in drie jaar wordt afgeschreven, wordt jaarlijks een derde van de aanschafwaarde afgeschreven. Variabele kosten: deze kosten van een IT-product of -dienst zijn wel afhankelijk van de hoogte van de productie, bijvoorbeeld de kosten van papier en toner voor de printer. Hoe meer er geprint wordt, hoe hoger het verbruik van papier en toner. Ook het inhuren van extern personeel is een voorbeeld van variabele kosten: hoe drukker het is, hoe meer personeel er wordt ingehuurd.
8. Capitalkosten: dit zijn de aanschafkosten van IT-productiemiddelen die meerdere jaren worden gebruikt. De kosten worden over meerdere jaren afgeschreven. Alleen de periodieke afschrijving wordt tot de kosten gerekend. Revenuekosten: ook wel operationalkosten, dit zijn regelmatige kosten waar geen IT-productiemiddel tegenover staat, bijvoorbeeld verzekeringen, onderhoudscontracten en licenties.
9. Hardwarekosten, softwarekosten, personeelskosten, huisvestingskosten, uitbestedingskosten en overdraagbare kosten.
10. Budgeting, accounting en charging.
11. Budgeting is het vaststellen van het budget voor een vooraf overeengekomen periode.
12. Incremental en zero-based.
13. Het identificeren van de kosten.
14. Communication of information, pricing flexibility en notational charging.
15. Cost Plus: het verrekenen van de gemaakte kosten plus een winstopslag. Going Rate: diensten met standaard prijsafspraken. Target Return: diensten waarvoor van tevoren is vastgesteld wat ze moeten gaan opbrengen. What the market will bear: de prijzen zijn in verhouding met de prijzen in de markt. Negotiated Contract Price: over de prijzen van diensten wordt onderhandeld met de klant.
16. De accountmanager is verantwoordelijk voor het relatiebeheer met de klant, het adviseren van de klant bij vraagstellingen of problemen, en draagt zorg voor de nakoming van gemaakte (eventueel contractuele) afspraken met de klant.
17. Financial Management rapporteert aan de klant, aan Service Level Management en aan het management. Het geconstateerde verbruik van IT-diensten wordt aan de klant doorgegeven of gefactureerd. Service Level Management is vooral geïnteresseerd in de uitgaven per klant, de gebruikte charging- en accountingmethoden en de geschillen met de

- klant. Aan het IT-management wordt gerapporteerd over de totale kosten en baten van de IT-dienstverlening, de kosten per afdeling en de ruimte voor toekomstige investeringen.
18. Invoering van het proces Financial Management heeft zowel voordelen voor de klant als voor de IT-afdeling. De IT-afdeling is door de invoering van dit proces in staat om de kosten te identificeren, te classificeren en te berekenen. Het stelt de IT-afdeling in staat om alle gemaakte kosten terug te krijgen van de klant en investeringsplannen te maken die gebaseerd zijn op het terugwinnen van de kosten. Budgeting en accounting stellen de IT-manager in staat om zakelijke beslissingen te nemen over IT-diensten en investeringen daarin. Charging stelt het IT-management in staat om alle IT-kosten terug te winnen door ze te relateren aan het gebruik. Bovendien kan het klantgedrag worden bijgestuurd door tarieven voor piek- en daluren in te voeren. Hiermee krijgt het IT-management een middel in handen waarmee klantgedrag kan worden (bij)gestuurd.
19. Gebrekkige acceptatie bij de klant, die niet gewend is om te betalen voor IT-diensten. Gebrek aan betrokkenheid bij het IT-management, waardoor het proces niet serieus wordt genomen. Er zijn weinig medewerkers beschikbaar met een gecombineerde financiële- en IT-achtergrond. Het is moeilijk om informatie te achterhalen van niet-IT-diensten. De benodigde investeringen voor de ontwikkeling van informatiesystemen zijn moeilijk te realiseren.
20. Service level management, capacity management en configuration management.

**Waar/niet waar:**

1. Niet waar
2. Niet waar
3. Waar
4. Waar
5. Waar
6. Waar
7. Niet waar
8. Waar
9. Niet waar
10. Waar
11. Waar
12. Waar
13. Waar

**Meerkeuzeopgaven:**

1. B
2. D
3. D
4. D
5. D
6. A
7. C
8. D
9. C
10. A



## Hoofdstuk 13 Availability Management

### Vragen en opdrachten met betrekking tot de casus:

1. Gebruikers, klanten, IT-afdeling, interne en externe leveranciers.
2. BIS, MS-Office, internet, e-mail.
3. Reliability = betrouwbaarheid, de mate waarin de klant van Bikefun kan vertrouwen op de juistheid, volledigheid, tijdigheid en geoorloofdheid van de verwerking van zijn reserveringsgegevens door BIS. Serviceability: de contractuele verplichtingen van Bikefun met de externe dienstverleners zoals vastgelegd in underpinning contracts. Maintainability: de mate waarin onderdelen van de IT-infrastructuur, bijvoorbeeld BIS, kunnen worden hersteld naar de operationele status na een storing. Recovery: herstelbaarheid, de inspanning die nodig is om een dienst als BIS te herstellen als deze uitvalt.
4. Incident Management levert aan Availability Management rapportages over hersteltijden, reparatietijden, etc. Problem Management is direct betrokken bij het herkennen en oplossen van de oorzaken van niet-beschikbaarheid van IT-diensten.
5. Om een beschikbaarheidsplan op te kunnen stellen moet Jaap eerst de beschikbaarheidsbehoeften vaststellen. Daarna kan hij de beschikbaarheid en de herstelbaarheid ontwerpen. Ook de beveiligingsaspecten moeten worden onderzocht. Na het plannen van de onderhoudsactiviteiten stelt Jaap een plan op voor het meten van de diverse beschikbaarheidsaspecten. Tenslotte resulteert dit alles in een beschikbaarheidsplan.
6. Een meerjarenplanning voor het verbeteren van de beschikbaarheid waarin de huidige situatie wordt weergegeven, richtlijnen staan voor bestaande diensten en voorstellen voor verbeteringen.
7. Bijvoorbeeld: als de normale datacommunicatielijn en de reserveverbinding het begeven, dan is het netwerk buiten werking. Als de server, of BIS, of het netwerk plat ligt, dan is het informatiesysteem BIS buiten werking. Als dit binnen de service-uren gebeurt, is de dienst niet beschikbaar.
8. Het beschikbaarheidspercentage is dan  $(48+4-3)/52*100\% = 94\%$ .
9. Het beschikbaarheidspercentage is dan  $(48+4-1)/52*100\% = 98\%$ .
10. Het beschikbaarheidspercentage is dan  $0,98*0,99*0,97*0,98*100\% = 92\%$ .
11. Het beschikbaarheidspercentage van de server wordt dan  $(1-(1-0,97)*(1-0,97)*100\%) = 99,91\%$ . De totale beschikbaarheid is dan  $(0,98*0,99*0,9991*0,98)*100\% = 95\%$ .
12. De totale beschikbaarheid is  $0,98*0,95*100\% = 93\%$ .
13. Het belangrijkste voordeel van Availability Management is dat de IT-afdeling van Bikefun in staat is om IT-diensten te ontwerpen die voldoen aan de met de klant overeengekomen beschikbaarheidseisen. Andere voordelen staan op blz. 205.

**Open vragen:**

1. Het kosteneffectief bewaken van de met de klant in het SLA overeengekomen beschikbaarheid van de IT-dienstverlening.
2. Aantal storingen, aantal wijzigingen, aard van de apparatuur, betrouwbaarheid van de apparatuur, uitwijkvoorzieningen, back-up faciliteiten, contracten met interne IT-dienstverleners en contracten met leveranciers.
3. Reliability: betrouwbaarheid, de mate waarin de klant kan vertrouwen op de juistheid, volledigheid, tijdigheid en geoorloofdheid van de gegevensverwerking. Serviceability: onderhoudsverplichting, de contractuele verplichtingen met de externe dienstverleners zoals vastgelegd in underpinning contracts. Maintainability: onderhoudbaarheid, de mate waarin onderdelen van de IT-infrastructuur kunnen worden hersteld naar de operationele status na bijvoorbeeld een storing. Recoverability: herstelbaarheid, de inspanning die nodig is om een dienst te herstellen als deze uitvalt. Hieronder vallen ook de detectie van fouten, het stellen van een diagnose, het zelf herstellen van fouten en het hervatten van de dienstverlening.
4. De activiteiten van Availability Management zijn planningsgericht en controlegericht en resulteren in een beschikbaarheidsplan, een meerjarenplan waarin de huidige situatie wordt beschreven en voorstellen worden gedaan voor de verbetering van de beschikbaarheid van IT-componenten.
5. Bepalen van de beschikbaarheidsbehoeften, ontwerpen van de beschikbaarheid, ontwerpen van de herstelbaarheid, aandachtspunten beveiliging, managen van onderhoudsactiviteiten.
6. De MTTR (Mean Time To Repair): de gemiddelde storingstijd. De MTBF (Mean Time Between Failures): het gemiddelde storingsvrije interval. De MTBSI (Mean Time Between System Incidents): de gemiddelde tijd tussen incidenten, dit is de som van MTTR en MTBF.
7. Een meerjarenplanning voor het verbeteren van de beschikbaarheid waarin de huidige situatie wordt weergegeven, richtlijnen staan voor bestaande diensten en voorstellen voor verbeteringen.
8. CFIA: Component Failure Impact Analysis, FTA: Fault Tree Analysis, CRAMM: de CCTA Risico Analyse en Management Methode, SOA: System Outage Analysis, TOP: Technical Observation Post.
9. Door van de overeengekomen servicetijd de storingstijd tijdens de serviceuren af te trekken en vervolgens te delen door de overeengekomen servicetijd en te vermenigvuldigen met 100%.
10. Bij een dienst die uit verschillende seriële onderdelen bestaat moeten de beschikbaarheidspercentages van de componenten worden vermenigvuldigd.
11. Bij parallelle componenten moet de niet-beschikbaarheid van de parallelle componenten worden vermenigvuldigd om de totale beschikbaarheid van de component te berekenen.
12. Availability Management rapporteert regelmatig aan de klant over de beschikbaarheid van IT-diensten. Deze rapportages bevatten gegevens over het niet-beschikbaar zijn van een dienst in termen van MTTR, MTBF en MTBSI. Andere onderwerpen waarover gerapporteerd wordt zijn aantallen storingen en totale tijdsduur van niet-beschikbaarheid. Bij de rapportages is het belangrijk om uit te gaan van de optiek van de klant: voorop staat de beschikbaarheid van de vitale bedrijfsfuncties, de businessapplicaties en de gegevens.
13. Naar de procesmanager wordt gerapporteerd over zaken als detectietijden, reactietijden, reparatietijden, hersteltijden, toegepaste methoden en technieken en gerealiseerde beschikbaarheid afgezet tegen de in het SLA overeengekomen beschikbaarheid.
14. Het is lastig om de balans aan te geven tussen de kosten van beschikbaarheid en niet-beschikbaarheid. Er wordt een te hoge beschikbaarheid nagestreefd, waarbij de kosten niet

in verhouding staan tot de opbrengsten. Beschikbaarheid wordt vertaald in een opsomming van technische details die de klant niets zeggen. De verantwoordelijkheid voor de beschikbaarheid wordt verdeeld over verschillende procesmanagers en lijnmanagers. Het ontbreekt aan draagvlak voor het aanstellen van een procesmanager. Het ontbreken van de juiste resources en middelen om te kunnen meten en rapporteren. Aansturing van interne en externe leveranciers is moeilijk.

15. De voordelen van de invoering van Availability Management voor de klant zijn: het creëren van een focus op de beschikbaarheid van de belangrijkste business-processen van de klant, het verleggen van de nadruk van foutherstel naar serviceverbetering, het beschikken over methoden en technieken om alle aspecten van beschikbaarheid te berekenen, het hebben van een vast aanspreekpunt binnen de organisatie over de beschikbaarheid van IT-diensten, het zeker stellen dat nieuwe producten en diensten voldoen aan de met de klant overeengekomen eisen met betrekking tot de beschikbaarheid, het bewaken en monitoren van alle beschikbaarheidsnormen, zodat de beschikbaarheid kan worden verbeterd, het nemen van correctieve maatregelen bij niet-beschikbaarheid, het afnemen van het aantal momenten van niet-beschikbaarheid en het afnemen van de duur van de niet-beschikbaarheid.
16. Het belangrijkste voordeel van de invoering van Availability Management voor de IT-afdeling is dat ze in staat is om IT-diensten te ontwerpen die voldoen aan de met de klant overeengekomen beschikbaarheidseisen.
17. Availability Management heeft relaties met de meeste andere ITIL-processen: de relatie met Service Level Management springt het meest in het oog, omdat daar de afspraken met de klant met betrekking tot de beschikbaarheid contractueel worden vastgelegd in een SLA, Configuration Management levert de noodzakelijke gegevens over de componenten van de IT-infrastructuur, incident Management levert aan Availability Management rapportages over hersteltijden, reparatietijden, etc. Problem Management is direct betrokken bij het herkennen en oplossen van de oorzaken van niet-beschikbaarheid van IT-diensten, Availability Management informeert Change Management over de onderhoudsaspecten van nieuwe diensten en doet wijzigingsvoorstellen om de beschikbaarheid te vergroten, Availability Management levert aan Security Management belangrijke informatie over de vertrouwelijkheid, de integriteit en de beschikbaarheid van (nieuwe) IT-diensten. IT Service Continuity Management geeft aan Availability Management informatie door over de kritische bedrijfsprocessen en over de herstelopties en uitwijkmogelijkheden na een calamiteit. Availability Management speelt aan Capacity Management informatie door over de beschikbaarheidseisen van de klant en de gevolgen die dit kan hebben voor de aanpassing van de capaciteit van de onderdelen van de IT-infrastructuur.

**Waar/niet waar:**

1. Waar
2. Waar
3. Niet waar, niet altijd maar volgens de afspraken die in het SLA staan.
4. Waar
5. Niet waar
6. Niet waar
7. Waar
8. Niet waar
9. Niet waar
10. Waar
11. Waar
12. Waar
13. Niet waar
14. Niet waar
15. Waar

**Meerkeuzeopgaven:**

1. C, in alle drie de genoemde contracten worden afspraken gemaakt met betrekking tot de beschikbaarheid.
2. Het juiste antwoord staat er niet bij: resilience
3. C
4. C
5. D, zie bladzijde 196 en verder
6. A
7. C
8. B, zie bladzijde 200
9. A, zie bladzijde 201, maatregelen horen bij risicomanagement.
10. A,  $2/40$  is 5%
11. A,  $0,95 * 0,98 * 0,99 * 100\% = 92\%$
12. B,  $(1 - (0,97 * 0,98)) * 0,98 * 0,99$

## Hoofdstuk 14 Capacity Management

### Vragen en opdrachten met betrekking tot de casus:

1. De werkstations hebben te weinig geheugen, de capaciteit van de datacommunicatie laat te wensen over, de harde schijven van de servers hebben te weinig capaciteit, een printer wordt te intensief gebruikt, terwijl twee andere printers niet worden gebruikt.
2. Jaap kan in het kader van het subproces Business Capacity Management de volgende activiteiten uitvoeren: onderkennen van de capaciteitsbehoeften van de klant, geven van aanbevelingen voor de aanschaf van nieuwe hardware en software met een performance- of capaciteitsaspect, bijwerken van de CDB met de technische specificaties van nieuw aangeschafte of gewijzigde CI's, aanpassen van de SLA's met betrekking tot nieuw aangeschafte of verbeterde CI's, opnieuw onderhandelen met de klant over de SLA's.
3. Het bijsturen van de vraag naar capaciteit, bijvoorbeeld door het verminderen van piekbelastingen en het stimuleren van het gebruik tijdens daluren.
4. Het identificeren en begrijpen van de capaciteit en het gebruik van ieder onderdeel van de IT-infrastructuur door informatie over het gebruik van deze onderdelen te verzamelen en het effect van wijzigingen in het gebruik van de diensten te verzamelen. Tevens kan Resource Capacity Management onderzoek doen naar de ontwikkeling van nieuwe technologieën en de manier waarop deze kunnen worden ingezet om de business te ondersteunen.
5. In het kader van het subproces Application Sizing probeert Capacity Management van de leverancier duidelijkheid te krijgen over de hardware-eisen van nieuwe applicaties.
6. In het capaciteitsplan moet in ieder geval de omvang van de huidige capaciteit binnen de IT-infrastructuur aan de orde komen en moet nadat de bedrijfsstrategie en -plannen zijn geraadpleegd een voorspelling over het toekomstige gebruik van resources die nodig zijn om de bedrijfsactiviteiten optimaal te ondersteunen worden gedaan. In het capaciteitsplan kunnen ook aanbevelingen worden opgenomen omtrent de benodigde hoeveelheid resources, de kosten, de voordelen, de impact op de bedrijfsprocessen, etc.
7. Jaap kan in het kader van Application Sizing voorspellingen doen over de hardware die nodig is voor nieuwe of aangepaste applicaties. De voorspellingen bevatten gegevens over de te verwachten prestatieniveaus, de benodigde hardware en de kosten. Application Sizing is vooral betrokken bij de beginfase van de ontwikkeling of aanpassing van software, bijvoorbeeld in de projectinitiatiefase, omdat dan een goed overzicht van de benodigde hardware en de kosten nodig is om met het ontwikkeltraject te kunnen starten.
8. In de Capacity Database (CDB) kunnen allerlei technische en zakelijke gegevens over de capaciteit van de onderdelen van de IT-infrastructuur worden opgenomen.
9. Uitbreiden van het intern geheugen van de werkstations, beter verdelen van de capaciteit over de beschikbare serviceuren door het verminderen van de piekbelastingen en het stimuleren van het gebruik tijdens daluren.
10. De SLA's moeten worden aangepast met betrekking tot de nieuw aangeschafte of verbeterde CI's en

**Open vragen:**

1. Het tegen verantwoorde kosten beschikbaar stellen van de juiste capaciteit aan IT-middelen die voorziet in de huidige en toekomstige behoeften van de klant.
2. Performance Management is het proces van meten, bewaken en bijstellen van de prestaties van de onderdelen van de IT-infrastructuur. Demand Management is vraagbeheer, het bijsturen van de vraag naar de capaciteit.
3. De wet van Moore: de capaciteit van elke nieuw ontwikkelde geheugenchip is dubbel zo groot als zijn voorganger en deze verdubbeling vindt ongeveer een keer per anderhalf jaar plaats. De wet van Parkinson: data zal altijd de beschikbare opslagruimte vullen, met andere woorden elke uitbreiding van de capaciteit zal na verloop van tijd worden benut, hetgeen tot nieuwe capaciteitsproblemen leidt.
4. Hardware als pc's en Servers, datacommunicatieapparatuur als bridges, routers, switches en gateways, randapparatuur als printers en opslagfaciliteiten, software: zowel systeemsoftware als applicatiesoftware, personeel: niet het 'normale' personeelsbeleid, maar vooral die gevallen waarbij een gebrek aan personeel leidt tot prestatieproblemen.
5. Business Capacity Management, Service Capacity Management en Resource Capacity Management.
6. Identificatie van en tot overeenstemming komen over de SLR's, ontwerp, aanschaf of verbetering van nieuwe diensten, update van CMDB en CDB, verificatie SLA en het aanpassen van het SLA.
7. Monitoring, analyse, implementatie, vullen van de CDB, demand management, modellering, application sizing en het opstellen van een capaciteitsplan.
8. Het bijsturen van de vraag naar capaciteit, bijvoorbeeld door het verminderen van piekbelastingen en het stimuleren van het gebruik tijdens daluren.
9. Trendanalyse, analytisch modelleren, simulatie en baseline.
10. Het bepalen van de hardwarecapaciteit van nieuwe of gewijzigde applicaties.
11. Een beeld van de omvang van de huidige capaciteit en een voorspelling over het toekomstig gebruik van resources.
12. Het ontwerpen van het netwerk; de configuratie van computersystemen; de configuratie van servers. Het beheren van de prestatiekenmerken van applicaties; het netwerk; de prestatiekenmerken van het netwerk; de server; prestatiekenmerken van de server; van systemen voor gegevensopslag; van de beschikbaarheid van gegevens en het bepalen van het onderhoud op de technische infrastructuur.
13. Beter inspelen op de capaciteitsbehoeften van de klant door voortdurende monitoring van de capaciteit van de onderdelen van de IT-infrastructuur. Vermindering van incidenten en problemen die te wijten zijn aan gebrek aan capaciteit. Betrouwbare voorspellingen over de capaciteitsbehoeften van de klant. Kosteneffectief gebruik van IT-middelen omdat vraag en aanbod in evenwicht zijn. Efficiënter benutten van de huidige capaciteit en het beter inspelen op de toekomstige capaciteitsbehoeften van de klant. Voorkomen van urgente wijzigingsvoorstellen door de verkeerde capaciteitsinschatting.
14. De verantwoordelijkheid over Capacity Management is verspreid over verschillende disciplines, vaak ontbreekt het aan een centraal aanspreekpunt voor capaciteitsvraagstukken. Te hoge verwachtingen van nieuwe applicaties van ontwerpers, opdrachtgevers en klanten vanwege onvoldoende inzicht in de technische mogelijkheden. Leveranciers verstrekken vaak verkeerde gegevens over de benodigde capaciteit en geven vaak een te optimistisch beeld van de werkelijke prestaties van een systeem. Problemen bij de implementatie van Capacity Management in complexe, gedistribueerde omgevingen, waarbij door de vele platforms en koppelingen vele performance-afhankelijkheden voorkomen. Het is vaak moeilijk om aan de juiste gegevens voor bijvoorbeeld het capaciteitsplan te komen omdat de gegevens verspreid zijn over

verschillende disciplines, de plannen van de business niet concreet genoeg en de toekomstverwachting van de klant niet duidelijk zijn. Het enige wat er dan op zit, is een zo goed mogelijke schatting te maken en deze regelmatig bij te stellen.

**Waar/niet waar:**

1. Niet waar, het tegen verantwoorde kosten beschikbaar stellen van de juiste capaciteit aan IT-middelen.
2. Waar
3. Niet waar
4. Niet waar
5. Waar
6. Waar, zie blz 216 onderaan
7. Waar, zie blz 220
8. Waar
9. Niet waar
10. Niet waar, geeft ook een beeld van de huidige omvang.
11. Waar

**Meerkeuzeopgaven:**

1. C
2. A
3. C, zie blz. 217
4. D
5. B
6. D
7. B
8. B, zie blz. 221
9. D
10. B

## Hoofdstuk 15 IT Service Continuity Management

### Vragen en opdrachten met betrekking tot de casus:

1. Storing, brand, inbraak, virusaanval, hacking.
2. Er is al een projectorganisatie opgezet.
3. Verstrekken van inlichtingen, boeken van reizen en vakanties, verhuur van fietsen, versturen van folders, beantwoorden van e-mail berichten.
4. Binnen Bikefun heeft BIS een hoge waarde, er zijn veel bedreigingen voor BIS, bijvoorbeeld een brand in de computerruimte, waarvoor de kwetsbaarheid groot is, want na een fikse brand is er niks meer over van de server en van BIS. Door voorzorgsmaatregelen te nemen, bijvoorbeeld regelmatig back-ups te maken en deze op te slaan in een brandvrije kluis worden de risico's beheersbaar en wordt BIS beschermd.
5. Als de centrale server waarop BIS staat, bijvoorbeeld door een brand uitvalt, vormt dat een grote bedreiging voor de continuïteit het bedrijfsproces. In combinatie met een grote kwetsbaarheid, want als er brand uitbreekt raakt de server ernstig beschadigd, zorgt dat voor een groot risico.
6. Een uitgebreide back-up en recovery-strategie; de eliminatie van zogenaamde “single points of failure” als een enkele stroomvoorziening zonder noodstroom; het uitbesteden van diensten aan meer dan een dienstverlener; het opzetten van veerkrachtige IT-systemen en netwerken die tegemoet komen aan de al maar toenemende behoeften van de business; de verbeterde toegangsbeveiliging door gebruik te maken van bijvoorbeeld smartcards; betere procedures als Change Management om de kans op fouten en storingen in de IT-infrastructuur te verkleinen.
7. Handmatige work-arounds, wederzijdse afspraken met een andere organisatie en een warme start op een andere locatie in het land.
8. Een calamiteitenplan, een uitwijkplan, een continuïteitsplan, een schadebeoordelingsplan, een herstelplan, een vital records plan en een crisis management en PR-plan.
9. Opleiding en bewustwording van de medewerkers, training van IT-personeel, review en audit van alle onderdelen en producten van het ITSCM-proces, testen om te zien of de plannen nog werken, Change Management beoordeelt van wijziging in de IT-infrastructuur de gevolgen voor de herstelplannen en past deze aan indien nodig, controle op de kwaliteit van alle betrokken producten.
10. De beslissing om bij een calamiteit al of niet over te stappen op de contingencyplannen moet worden genomen door een crisisteam, waarin zowel directieleden zitten als managers van de bij de calamiteit betrokken afdelingen. Als besloten wordt om de contingencyplannen in werking te stellen, moet dit snel met alle betrokkenen worden overlegd. Een telefooncirkel kan daarbij uitkomst bieden.



**Open vragen:**

1. Het ondersteunen van Business Continuity Management bij het nemen van preventieve maatregelen om calamiteiten zoveel mogelijk te voorkomen of de impact van calamiteiten op de bedrijfsprocessen te verminderen.
2. IT Service Continuity Management (ITSCM) vormt een integraal onderdeel van Business Continuity Management (BCM), wat betekent dat eerst de doelstellingen van de business met betrekking tot het overkoepelende continuïteitsbeheer moeten worden vastgesteld. ITSCM ondersteunt het overkoepelende BCM, dus eerst moet de scope van ITSCM worden afgeleid van de doelstellingen van de business.
3. Een calamiteit is een onverwachte verstoring van een service of systeem met aanzienlijke gevolgen voor de continuïteit van de dienstverlening.
4. Initiatie, uitgangspunten en strategie, implementatie en operationeel management.
5. Bepalen van het beleid, specificeren van aandachtsgebieden en scope, toewijzen van middelen en het inrichten van een projectorganisatie.
6. Het doel van Business Impact Analyse (BIA) is te onderzoeken wat de kritische bedrijfsprocessen zijn en wat het potentiële verlies of de potentiële schade is die aan de organisatie wordt toegebracht door het uitvallen van de bedrijfskritische systemen.
7. Met behulp van CRAMM kan een inschatting worden gemaakt van de bedreigingen en de mate waarin een organisatie kwetsbaar is voor die bedreigingen. Door met behulp van CRAMM een risicoanalyse uit te voeren kan worden onderzocht welke voorzorgsmaatregelen tegen de bedreigingen kunnen worden genomen.
8. Aan de hand van de risicotabel kan het risico voor elk productiemiddel worden beoordeeld in termen van de ermee verbonden bedreigingen en kwetsbaarheden. Door gebruik te maken van de risicotabel kan de kans van het optreden van een bepaald risico voor een bepaald productiemiddel worden onderzocht.
9. Een uitgebreide back-up en recovery-strategie; de eliminatie van zogenaamde “single points of failure” als een enkele stroomvoorziening zonder noodstroom; het uitbesteden van diensten aan meer dan een dienstverlener; het opzetten van veerkrachtige IT-systemen en netwerken die tegemoet komen aan de al maar toenemende behoeften van de business; de verbeterde toegangsbeveiliging door gebruik te maken van bijvoorbeeld smartcards; betere procedures als Change Management om de kans op fouten en storingen in de IT-infrastructuur te verkleinen.
10. Omdat niet voor alle risico's preventieve maatregelen kunnen worden genomen, zijn er aanvullend herstelopties nodig om de dienstverlening zo snel mogelijk te herstellen als een calamiteit zich toch voordoet.
11. Niets doen, handmatige work-arounds, reciprocal agreements, gradual recovery naar een vaste of portable ruimte, intermediate recovery naar een interne, een externe of een portable ruimte en immediate recovery.
12. Het inrichten van de organisatie en ontwikkelen van implementatieplannen; het implementeren van stand-bymaatregelen; het implementeren van risico-reductiemaatregelen; het ontwikkelen van IT-herstelplannen; het ontwikkelen van procedures en een initiële test.
13. Opleiding en bewustwording van de medewerkers, training van IT-personeel, review en audit van alle onderdelen en producten van het ITSCM-proces, testen om te zien of de plannen nog werken, Change Management beoordeelt van wijziging in de IT-infrastructuur de gevolgen voor de herstelplannen en past deze aan indien nodig, controle op de kwaliteit van alle betrokken producten.
14. De beslissing om bij een calamiteit al of niet over te stappen op de contingencyplannen moet worden genomen door een crisisteam, waarin zowel directieleden zitten als managers van de bij de calamiteit betrokken afdelingen. Als besloten wordt om de

contingencyplannen in werking te stellen, moet dit snel met alle betrokkenen worden overlegd. Een telefooncirkel kan daarbij uitkomst bieden.

15. Zie de tabel op bladzijde 244.
16. Het belangrijkste proces waarmee wordt samengewerkt is Service Level Management, omdat in een SLA de verplichtingen worden opgenomen met betrekking tot ITSCM. Availability Management ondersteunt ITSCM door het ontwikkelen en implementeren van voorzorgsmaatregelen, bovendien maakt ITSCM gedeeltelijk gebruik van dezelfde methoden en technieken als Availability Management en Capacity Management (CRAMM). Change Management zorgt ervoor dat de ITSCM-plannen actueel blijven door wijzigingsvoorstellen te beoordelen en te autoriseren. Configuration Management ondersteunt ITSCM door het vastleggen van gegevens over baselines en alle andere onderdelen van de IT-infrastructuur. Capacity Management ondersteunt ITSCM door de juiste middelen beschikbaar te stellen.

**Waar/niet waar:**

1. Niet waar
2. Niet waar, een calamiteit is een onverwachte verstoring van een service of een systeem met aanzienlijke gevolgen voor de continuïteit van de dienstverlening.
3. Niet waar
4. Niet waar
5. Waar
6. Niet waar, CRAMM volgt na de Business Impact Analyse
7. Waar
8. Waar
9. Waar
10. Waar
11. Waar
12. Niet waar, het crisisteam wordt gevormd door de directie en het management van de bij de calamiteit betrokken afdelingen.
13. Waar, de recovery wordt uitgevoerd door de teamleiders samen met de teamleden.

**Meerkeuzeopgaven:**

1. B
2. C
3. B
4. C
5. C
6. B
7. B
8. B
9. A
10. B
11. C
12. B
13. C
14. B
15. C

## Hoofdstuk 16 Security Management

### Vragen en opdrachten met betrekking tot de casus:

1. Vertrouwelijkheid: de mate waarin bij Bikefun de toegang tot en het gebruik van de gegevens van Bikefun beperkt is tot degenen die daarvoor zijn geautoriseerd.  
Betrouwbaarheid: de mate waarin bij Bikefun de toegang tot en het gebruik van de gegevens van Bikefun beperkt is tot degenen die daarvoor zijn geautoriseerd in combinatie met de juistheid, correctheid en volledigheid van de in het BIS opgeslagen informatie en de mate waarin de informatie op het juiste moment beschikbaar is voor de gebruikers ervan.
2. Hij wil daarmee waarschijnlijk inzicht krijgen in het aantal en de soort beveiligingsincidenten, waarmee hij vervolgens het management kan overtuigen van de noodzaak van het proces Security Management. Tevens wordt hiermee de bewustwording van management en medewerkers gestimuleerd.
3. In ieder geval wordt niet zorgvuldig omgesprongen met de grondwet: de eerbiediging van de persoonlijke levenssfeer en de WBP: de wet op de bescherming van persoonsgegevens.
4. Ja, want de betrouwbaarheid (vertrouwelijkheid, integriteit en beschikbaarheid) van de informatievoorziening wordt erdoor verstoord. Daardoor kan schade ontstaan, die moet worden hersteld.
5. Er werden wetten overtreden, onder andere de WBP en de betrouwbaarheid en goede naam van Bikefun werden erdoor aangetast.
6. Het Itil-proces Security Management, de Code voor Informatiebeveiliging en de Code of Practice for Information Security Management.
7. Preventieve maatregelen, detectieve maatregelen, repressieve maatregelen en correctieve maatregelen.
8. Eerst moet beleid worden ontwikkeld: wat zijn de doelstellingen van de informatiebeveiliging?
9. Allereerst moet een beleidsdocument worden opgesteld met doelen voor beveiliging. Vervolgens moeten verantwoordelijkheden worden toegewezen en moet het personeel worden getraind. Er moet een rapportage worden opgezet over beveiligingsincidenten. Er moet op virussen worden gecontroleerd en er moet worden gereageerd op calamiteiten. Het onrechtmatig kopiëren van programmatuur en van informatie moet worden voorkomen. en bedrijfsdocumenten moeten worden beveiligd. Tenslotte moet worden voldaan aan wet- en regelgeving en moet er toezicht en controle worden uitgeoefend op de naleving van beleid en normen.
10. Er kunnen eigen beoordelingen worden gemaakt door de lijnmanagers en de procesmanagers; er kan een interne audit worden gehouden door een interne edp-auditor en er kan een externe audit worden gehouden door een externe edp-auditor.
11. De wensen en eisen van de klant en het resultaat van het subproces evaluatie en van voortschrijdend inzicht in de risico's die worden gelopen zijn de input voor het onderhoud van het SLA.
12. De Underpinning Contracts en de Operational Level Agreements.

**Open vragen:**

1. Met integriteit wordt bedoeld in hoeverre de informatie een correcte weergave is van de werkelijkheid. Integriteit bestaat uit de onderdelen: juistheid, correctheid en volledigheid.
2. De grondwet, de Wet computer criminaliteit (WCC), de Wet Bescherming persoonsgegevens (WBP), de Telecommunicatiewet en de Auteurswet.
3. Itil Security Management, de Code voor Informatiebeveiliging, de Code of Practice for Information Security Management en de VIR'94.
4. Beveiligingsbeleid, organisatie van de beveiliging, classificatie en beheer, personeel, fysieke beveiliging, computer en netwerkbeheer, toegangsbeveiliging, systeemontwikkeling en onderhoud, continuïteitsplanning en toezicht.
5. Er moet eerst een beleidsdocument worden opgesteld met doelen voor beveiliging. Vervolgens moeten verantwoordelijkheden worden toegewezen en moet het personeel worden getraind. Er moet een rapportage worden opgezet over beveiligingsincidenten. Er moet op virussen worden gecontroleerd en er moet worden gereageerd op calamiteiten. Het onrechtmatig kopiëren van programmatuur en van informatie moet worden voorkomen. en bedrijfsdocumenten moeten worden beveiligd. Tenslotte moet worden voldaan aan wet- en regelgeving en moet er toezicht en controle worden uitgeoefend op de naleving van beleid en normen.
6. Dreiging, incident, schade en herstel.
7. Preventieve maatregelen moeten voorkomen dat een dreiging tot een incident leidt. Detectieve maatregelen zijn bedoeld om een beveiligingsincident op te sporen. Repressieve maatregelen moeten de negatieve invloed van een incident minimaliseren. Correctieve maatregelen zijn bedoeld om de objecten te herstellen die zijn beschadigd.
8. Sturing, maken van een plan, implementatie, evaluatie, onderhoud en rapportage.
9. SLA, OLA en underpinning contract.
10. Classificatie en beheersing van IT-hulpmiddelen, personele beveiliging, veilig beheer en toegangsbeveiliging.
11. Verificatie van de naleving van beveiligingsbeleid en implementatie; beveiligingscontrole op it-systemen; opsporen en reageren op ongewenst gebruik van it-voorzieningen; uitvoeren van de securityaspecten van de overige edp-audits.
12. Alle informatiebeveiligingsplannen: SLA, OLA en UC.
13. Er wordt regelmatig aan de klant gerapporteerd over de geleverde beveiligingsdiensten.
14. Strategisch: de security officer. Tactisch: de security specialist. Operationeel: de beheerder informatiebeveiliging en de autorisatiebeheerder.
15. Over de voortgang van de invoering en de kwaliteit van de procesgang, bijvoorbeeld rapportages over de diverse contracten met interne (OLA) en externe leveranciers (Underpinning Contracts) en eventuele problemen daarmee, rapportages over beveiligingsplannen, actieplannen en eigen beleidsuitgangspunten, rapportages over de voortgang van de implementatie van de informatiebeveiliging: voortgang beveiligingsjaarplan, maatregelen, opleiding en status bewustwordingsprogramma. Rapportages over trends in beveiligingsincidenten, de resultaten van audits, reviews en interne controles en de identificatie van nieuwe bedreigingen.
16. Beveiligingsincidenten kunnen ernstige gevolgen hebben voor de continuïteit van de dienstverlening en kunnen escaleren tot calamiteiten. ITSCM is in zo'n geval verantwoordelijk voor het nemen van voorzorgsmaatregelen en uitwijkplannen en het zo snel mogelijk herstellen van de normale dienstverlening.

**Waar/niet waar:**

1. Waar
2. Niet waar, betrouwbaarheid is een combinatie van beschikbaarheid, integriteit en vertrouwelijkheid.
3. Waar
4. Niet waar
5. Waar
6. Niet waar, repressieve maatregelen moeten de negatieve invloed van een incident minimaliseren
7. Niet waar
8. Waar
9. Niet waar
10. Niet waar, de security officer is hiervoor verantwoordelijk
11. Waar

**Meerkeuzeopgaven:**

1. C
2. B
3. D
4. B
5. D, dreiging, detectie, schade, herstel, zie blz. 254
6. C, blz. 255
7. D
8. C
9. B
10. B

## Hoofdstuk 17 Beheer door derden

### Vragen en opdrachten met betrekking tot de casus:

1. Ja, focus op de kerntaken is een legitieme reden voor het uitbesteden van delen van IT-diensten.
2. Ja, de totale kosten van het uitbesteden kunnen te hoog zijn als ook de overgangskosten worden meegerekend. Er kan afhankelijkheid ontstaan van een externe organisatie en het beleid dat daar wordt gevoerd. Ondersteuning kan door een organisatie als een strategisch middel worden gezien waarvoor men zelf verantwoordelijk wil zijn, vooral als er veel nieuwe ontwikkelingen spelen. Het afstoten van eigen personeel kan sociale onrust veroorzaken of in strijd zijn met het personeelsbeleid.
3. Nee, er wordt nergens vermeld dat hij het fenomeen uitbesteding heeft bestudeerd via internet, literatuurstudie of ervaringen van anderen.
4. Detachering.
5. Outsourcing.
6. Niet allemaal, wel het technisch beheer en het applicatiebeheer.
7. Nee, het strategisch beheer kan moeilijk worden uitbesteed, de strategische aspecten van informatiesystemen horen bij de organisatie waar het informatiesysteem deel vanuit maakt.
8. Ja.
9. Wel het applicatiebeheer, niet het functionele onderhoud.
10. In grote lijnen wel.

### Open vragen:

1. Outsourcing, third party maintenance en detachering.
2. De organisatie wil zich alleen nog richten op de kerntaken, de 'core business'. Er wordt geen energie meer gestoken in taken die niet tot de kerntaken behoren. Doordat de apparatuur en het personeel deel gaan uitmaken van een groter geheel, zijn kostenbesparingen te bereiken. Voor het inkopen van grotere hoeveelheden apparatuur kunnen bijvoorbeeld makkelijker kortingen worden bedongen bij de leverancier. Er is onvoldoende kennis en ervaring aanwezig bij het eigen personeel, waardoor het toepassen van nieuwe technologieën stagneert. Het wordt mogelijk om beter te kunnen inspelen op verzoeken vanuit het gebruik, bijvoorbeeld de snelheid van verwerking. De inspanning die nodig is om het beheer verantwoord in te richten, is niet te realiseren met eigen personeel.
3. 1. Het formuleren van de doelstelling van het onderzoek: om welke delen van het beheer (functioneel, technisch of applicatiebeheer) gaat het en om welk niveau (strategisch, tactisch of operationeel)? 2. Het bestuderen van het fenomeen uitbesteding via internet, literatuurstudie of ervaringen van anderen. 3. Het in kaart brengen van het eigen beheer. Alle aspecten van het beheer worden in kaart gebracht: organisatie, personeel, materiële en financiële middelen. 4. Het uitwerken van enkele scenario's inzake mogelijke uitbesteding. Deze worden gehanteerd als alternatieven om sterke en zwakte vanuit verschillende invalshoeken te bepalen. 5. Het selecteren van potentiële bedrijven aan wie het beheer of aspecten ervan kunnen worden uitbesteed. 6. Aan de in stap vijf geselecteerde bedrijven wordt een reactie gevraagd over de in stap vier uitgewerkte scenario's. Dit gebeurt door het opstellen van offertes. Deze kunnen zowel globaal als gedetailleerd zijn, afhankelijk van de aard van de scenario's en de kennis van zaken van dat moment. Een indicatieve offerte is in deze fase voldoende. 7. Op basis van de in de vorige fase verkregen informatie wordt nu aan enkele potentiële bedrijven gevraagd om een of meer offertes uit te werken in een concrete offerte. 8. De offertes worden onderling vergeleken en vergeleken met het eigen beheer. 9. In deze fase wordt besloten welk

bedrijf voor uitbesteding in aanmerking komt. Dit kan ook betekenen dat geen bedrijf in aanmerking komt, waarna terug kan worden gegaan naar een van de eerdere stappen of beheer door derden wordt afgewezen. 10. Als in de vorige stap is besloten over te gaan tot uitbesteding, wordt in deze fase het contract opgesteld waarin de overgang naar uitbesteden en de financiering worden vastgelegd.

4. Tijdens het stappenplan moet het bij het beheer betrokken personeel expliciete aandacht krijgen in de vorm van voorlichting en het opstellen van een plan waarin wordt uitgelegd hoe met de personele consequenties wordt omgegaan.
5. Third party maintenance (TPM) duidt op het uitbesteden van het correctief en preventief onderhoud dat betrekking heeft op de apparatuur en de bijbehorende technische basisprogrammatuur en de bijbehorende technische voorzieningen.
6. Er geldt een (voorlopige) vacaturestop. Het ingehuurde personeel beschikt over een specialisme dat slechts beperkt beschikbaar is. Vacatures kunnen op korte termijn niet worden vervuld vanwege de krappe arbeidsmarkt. Apparatuurverplaatsingen naar nieuwe locaties vereisen inzet van extra personeel. De vervanging van zelf ontwikkelde beheerpakketten door extern ontwikkelde pakketten gebeurt onder supervisie van een externe projectleider.
7. De operationele beheertaken kunnen goed worden uitbesteed.
8. Beheer op strategisch niveau kan niet worden uitbesteed: de strategische aspecten van informatiesystemen horen bij de organisatie waar het informatiesysteem deel vanuit maakt.
9. Bij functioneel beheer komt van de drie vormen van beheer door derden alleen inhuren in aanmerking voor het beheer op operationeel en tactisch niveau.
10. Ja, alleen het strategisch niveau kan ook hier niet goed worden uitbesteed, het betreft de beleidsbepaling op het gebied van het technisch beheer, en dat moet binnen de eigen organisatie gebeuren.

**Waar/niet waar:**

1. Niet waar
2. Waar
3. Waar
4. Waar
5. Waar
6. Waar
7. Waar
8. Waar
9. Waar
10. Waar

**Meerkeuzeopgaven:**

1. A
2. B
3. A
4. A
5. C
6. C
7. C
8. C
9. C
10. A

## Hoofdstuk 18 Relatie met andere standaarden

### Vragen en opdrachten met betrekking tot de casus:

1. Kwaliteitsbeleid: investeren in kwaliteitsverbetering, inrichten van een kwaliteitssysteem, invoeren van standaarden als Prince2, ASL, CMM en INK, certificatie volgens ISO 9000.
2. ISO 9000 is een aanvulling op ISO 8402 en geeft een aantal IT-specifieke aanvullingen op ISO 8402. ISO 9000 speelt een belangrijke rol bij het begrijpen en gebruiken van de andere drie normen in de ISO 9000-serie en kan om die reden bij Bikefun worden ingevoerd.
3. Ongeveer op tussen niveau 2 en 3: bij Bikefun wordt gebruik gemaakt van een standaardmethode als Itil en overweegt men andere standaardmethoden in te voeren.
4. Voor alle mogelijke projecten: bijvoorbeeld de invoering van ISO.
5. CMM-niveau 3 kan door Bikefun in eerste instantie worden nagestreefd, omdat men op het punt staat om allerlei standaard methoden en technieken in te voeren.
6. De procesmatige aanpak, het public-domain karakter, het gebruik van best practices, de gemeenschappelijke (sub)processen: configuratiebeheer, wijzigingsbeheer, risicobeheer, en kwaliteitsbeheer.
7. Bijvoorbeeld de IT-afdeling van Bikefun maakt gebruik van standaarden als ITIL, terwijl de rest van de organisatie hier niet mee bekend is. Er kan zich dan een communicatieprobleem voor doen omdat de meer formele werkwijze van Itil botst met de informele werkwijze van de rest van de organisatie.
8. De procesmatige aanpak, het public-domainkarakter, het gebruik van best practices, de invulling van de processen op 3 niveaus: strategisch, tactisch en operationeel. Een aantal gemeenschappelijke processen: configuratiebeheer, incidentbeheer, capaciteitsbeheer, beschikbaarheidbeheer, continuïteitsbeheer, wijzigingsbeheer, programmabeheer en distributie, service level management, cost management en het instellen van een centraal aanspreekpunt voor de gebruiker: het serviceteam.
9. Het serviceteam kan binnen Bikefun het centrale aanspreekpunt voor de klant worden met betrekking tot alle vormen van beheer. Het serviceteam draagt dan de verantwoordelijkheid voor de integrale kwaliteit (technische en functionele) van de informatievoorziening aan de klant, zorgt voor het definiëren van de gewenste dienstverlening en houdt hierop toezicht. Het serviceteam coördineert onderlinge afspraken, controleert of deze worden nagekomen, en rapporteert hierover aan de klantorganisatie. Zo beheert het team de totale informatievoorziening: de ontwikkeling, de innovatie, het gebruik en de exploitatie.
10. Een organisatie die een kwaliteitssysteem ontwikkelt volgens een van bovengenoemde ISO-normen kan bij een erkend instituut een certificaatkeuring aanvragen. Als bij de keuring blijkt dat de kwaliteitsnormen goed worden toegepast, ontvangt een organisatie een kwaliteitscertificaat. Dit certificaat is een soort garantie dat de organisatie in staat is om kwalitatief goed werk af te leveren. Een IT-organisatie die een ISO 9001-certificaat heeft, wordt geacht volgens deze normen te werken.



**Open vragen:**

1. ISO 8402 geeft een definitie van alle begrippen die een rol spelen bij de beschrijving van een kwaliteitssysteem.
2. Het geheel aan eigenschappen en kenmerken van een product of dienst dat van belang is voor het voldoen aan vastgestelde of vanzelfsprekende behoeften.
3. Deze normen geven aan welke activiteiten in een organisatie moeten worden uitgevoerd om de kwaliteit van producten en diensten te waarborgen.
4. Initieel, herhaalbaar, gedefinieerd, bestuurd en geoptimaliseerd.
5. Nagaan hoever het bedrijf is gevorderd met het streven naar Total Quality Management. Interne en externe auditoren kunnen aan de hand van vragenlijsten nagaan hoe volwassen de verschillende onderdelen uit het INK-model zijn (nul-meting). Vervolgens kan een strategie worden ontwikkeld om de resultaten te verbeteren.
6. Productgeoriënteerd, procesgeoriënteerd, systeemgeoriënteerd, ketengeoriënteerd en de totale zorg voor kwaliteit.
7. Prince2 (Projects In Controlled Environments) is een gestandaardiseerde projectmanagementmethodiek waarin richtlijnen en hulpmiddelen worden gegeven voor het opstarten, initiëren, uitvoeren, beheersen en afsluiten van projecten.
8. Risicobeheer, kwaliteitsbeheer, configuratiebeheer en wijzigingsbeheer.
9. ASL bestaat uit een framework en een bibliotheek van best practices op het gebied van applicatiebeheer. Het framework geeft invulling aan een aantal applicatiebeheerprocessen op strategisch, tactisch en operationeel niveau.
10. Het ASL-framework bestaat net als Itil uit een aantal clusters van processen die de inrichting van een applicatiebeheerorganisatie beschrijven. Deze processen vertonen veel overeenkomsten met de gelijknamige ITIL-processen. Door het uitvoeren van de processen wordt net als bij ITIL op drie niveaus invulling gegeven aan de applicatiebeheerprocessen.
11. De procesmatige aanpak, het public-domainkarakter, het gebruik van best practices, de invulling van de processen op 3 niveaus: strategisch, tactisch en operationeel. Tevens hebben ze een aantal gemeenschappelijke processen: risicobeheer, kwaliteitsbeheer, configuratiebeheer en wijzigingsbeheer.
12. Het uitwerken van de bedrijfsprocessen, het procesmatig denken, het gebruik van standaarden, focus op de kwaliteit.
13. Processen als configuratiebeheer, wijzigingsbeheer en kwaliteitsbeheer komen zowel voor bij ITIL als bij Prince2 en ASL. Het is belangrijk deze gemeenschappelijke processen op elkaar af te stemmen.

**Waar/niet waar:**

1. Waar
2. Waar
3. Waar
4. Waar
5. Waar
6. Waar
7. Waar
8. Waar
9. Waar
10. Niet waar

**Meerkeuzeopgaven:**

1. A
2. A
3. A
4. B
5. B
6. D
7. A
8. C
9. A
10. A

## Hoofdstuk 22 Proefexamen 1:

1. D
2. C
3. C
4. B
5. D
6. C
7. B
8. A
9. D
10. A
11. D
12. A
13. C, zie tekening op bladzijde 126
14. B, beide codes lopen op, dus 3 is het hoogste
15. C
16. C
17. C, release management is uitvoeringsgericht, change management controle gericht.
18. B
19. A
20. D
21. B
22. B
23. A
24. B
25. A
26. A
27. A en C zijn beide goed, zie blz. 198
28. B
29. D
30. A
31. B
32. A, zie vraag 7
33. B
34. A
35. C
36. B
37. B
38. A,B,C zijn allemaal goed
39. A
40. A

## Proefexamen 2

1. A
2. C
3. D
4. C
5. B
6. A
7. A
8. A
9. C
10. B
11. B
12. A
13. D
14. D
15. D
16. C
17. A, dit is geen software
18. C
19. A
20. B
21. A
22. D
23. D, antwoord A is gedeeltelijk goed want beschikbaarheid is een aspect van betrouwbaarheid
24. B
25. A
26. D, capacity management richt zich vooral op de toekomst.
27. D
28. A
29. A
30. B
31. B, zie blz. 235
32. B
33. A
34. A
35. A, een transactie is meetbaar
36. C
37. B
38. A
39. B, de oorzaak is niet bekend
40. B