Disaster Recovery planning

Scriptie

Student: Mirthe van de Wildenberg
Studentnummer: 1610609
Onderwijsinstelling: Hogeschool Utrecht
Docentbegeleider: Dhr. L.M. Roeleveld

Bedrijf: Tsubakimoto Europe B.V.
Bedrijfsbegeleider: Dhr. C. Bruntink

Versie: 1.0
Datum: 14-12-2015

Innovation in Motion
TSUBAKI

Colofon

Datum
14-12-2015

Hogeschool Utrecht
Nijenoord 1
3552 AS Utrecht
T.: (088) 481 8283

Faculteit Natuur en Techniek
System and Network Engineering

Afstudeerperiode: *31 augustus tot en met januari 2016*

Docentbegeleider (2e examinator)
Dhr. L.M. Roeleveld
E.: leen.roeleveld@hu.nl

1e examinator
Dhr. H. van Nimwegen
E.: henk.vannimwegen@hu.nl

Student
Mirthe van de Wildenberg
1610609
E.: mirthe.vandewildenberg@student.hu.nl
T.: 06 10 414 353

TSUBAKIMOTO EUROPE B.V.
Aventurijn 1200
3316 LB Dordrecht
E.: info@tsubaki.eu
T.: (078) 620 4000
W.: www.tsubaki.eu

Bedrijfsbegeleider
Dhr. C. Bruntink (ICT Manager)
E.: cor.bruntink@tsubaki.eu
T.: 06 20 709 362

Voorwoord

Deze scriptie is tot stand gekomen in het kader van mijn afstudeerproject genaamd ‘Disaster Recovery planning’. Tijdens mijn vijf maanden durende afstudeerstage bij Tsubakimoto Europe B.V. heb ik een onderzoek uitgevoerd m.b.t. het realiseren van een ‘Disaster Recovery plan’. Het schrijven van de scriptie heb ik ervaren als een intensieve en zeer belangrijke laatste periode van mijn studentenleven. Dit resultaat symboliseert tevens de afsluiting van mijn vierjarige Bacheloropleiding 'System and Network Engineering' aan de Hogeschool te Utrecht.

De afstudeerperiode heb ik ervaren als een van de meest leerzame periodes uit mijn studie. Door mijn opgedane kennis en nieuwe ervaringen gedurende de afstudeerperiode heb ik mij beter kunnen ontwikkelen in mijn vakgebied. Daarnaast heb ik in de afgelopen maanden de ruimte gekregen veel nieuwe en interessante dingen bij te leren.

Tsubakimoto Europe B.V. is met zekerheid meer dan alleen een afstudeerbedrijf voor mij geweest. Ik wil hierbij dan ook graag de volgende mensen bedanken die mij tijdens mijn afstudeerproject hebben ondersteund en begeleid. Mijn eerste dankwoord gaat uit naar Cor Bruntink voor zijn betrokkenheid, inzet en goede ondersteuning tijdens de afstudeerperiode. Ik wil hem daarbij vooral graag bedanken voor de bijzonder leerzame stageplek die hij mij heeft geboden. Daarnaast wil ik ook graag Tim Vergauwen bedanken voor zijn ondersteuning en hulp gedurende het afstudeerproject. Zonder hun toewijding en enthousiasme durf ik met zekerheid te zeggen dat dit project lang niet zo succesvol was geweest.

Hierbij bedank ik ook Leen Roeleveld voor zijn tijd, adviezen en feedback die mij gedurende de afstudeerperiode goed op weg hebben geholpen.

Natuurlijk bedank ik hierbij ook alle andere collega’s van Tsubakimoto Europe B.V. voor hun interesse en de prettige werkomgeving waar ik de afgelopen maanden deel van heb mogen uitmaken.

Mirthe van de Wildenberg

Dordrecht, december 2015

“ Hope for the best
and prepare for the worst ”

- John Jay (1813)

Management samenvatting

Tsubakimoto Europe B.V. verzorgt de distributie van industriële aandrijfkettingen en aanverwante producten aan haar klanten. Om dit te realiseren is het essentieel dat de IT omgeving beschikbaar is, ook in het geval van calamiteiten. Hierbij is het noodzakelijk dat de verantwoordelijken weten hoe zij dienen te handelen in het geval van calamiteiten, en welke maatregelen ondernomen moeten worden om het risico op calamiteiten te minimaliseren en waar mogelijk te voorkomen. Om die reden wil Tsubakimoto Europe B.V. beschikken over een Disaster Recovery plan (DRP).

Om dit te verwezenlijken is er een onderzoek verricht naar het realiseren van een Disaster Recovery plan voor Tsubakimoto Europe B.V. Voorafgaand aan het onderzoek is middels een scope bepaald dat het Disaster Recovery plan zich zal richten op de IT systemen en componenten die de kritische bedrijfsprocessen ondersteunen. Gedurende het onderzoek stond de volgende onderzoeksvraag centraal: "***Welke maatregelen zijn noodzakelijk om enerzijds het risico op calamiteiten te minimaliseren en anderzijds adequaat in te grijpen bij calamiteiten?***".

Uit dit onderzoek is gebleken dat het, voorafgaand aan het realiseren van het Disaster Recovery plan, eerst helder moet zijn welke IT systemen en componenten de kritische bedrijfsprocessen ondersteunen. Wanneer dit in kaart is gebracht, kan vervolgens de risicoanalyse worden uitgevoerd waarin onder meer de calamiteiten worden omschreven die een fysieke impact hebben op de IT systemen en data. Naar aanleiding van de risicoanalyse zijn de correctieve en preventieve maatregelen omschreven die, samen met de herstelprocedures, aan bod komen in het Disaster Recovery plan.

Het beantwoorden van de deelvragen heeft bijgedragen aan het formuleren van een antwoord op de onderzoeksvraag. De onderzoeksvraag is tweedelig: *Welke maatregelen zijn noodzakelijk om enerzijds het risico op calamiteiten te minimaliseren [1] en anderzijds adequaat in te grijpen bij calamiteiten [2]?*

[1] Er zijn verschillende maatregelen die genomen kunnen worden om de risico's op calamiteiten te minimaliseren en mogelijk te voorkomen:

- Een virusaanval of onopzettelijk handelen door personeel, kan dataverlies veroorzaken. Om het risico op een virusaanval te minimaliseren, moet er meer bewustzijn onder het personeel worden gecreëerd. Om dataverlies te voorkomen, dienen regelmatiger back-ups uitgevoerd te worden.
- Uitval van IT apparatuur kan worden veroorzaakt door diefstal, brand of hardware falen. Door bij voorbaat vervangende IT apparatuur aan te schaffen, kan systeemuitval worden voorkomen. Daarnaast kan het risico op diefstal van IT apparatuur worden verminderd, door de stellingen in de server ruimtes te voorzien van een slot.
- Het risico op een stroomstoring of hardware falen kan worden geminimaliseerd door de IT apparatuur regelmatiger te onderhouden, waardoor potentiële defecten tijdig hersteld kunnen worden. Daarnaast dient verouderde hardware in gebruik te worden vervangen, wat het risico op hardware falen verminderd.

[2] De verantwoordelijken binnen Tsubakimoto dienen als volgt in te grijpen in het geval van calamiteiten; wanneer een calamiteit zich voordoet, dient eerst de ernst van de situatie te worden ingeschat. Wanneer het DRP in werking is getreden, moet de impact op de IT apparatuur (en eventueel data) worden vastgesteld. Hierbij dienen klanten en leveranciers op de hoogte te worden gebracht van de situatie. Afhankelijk van de situatie dienen maatregelen genomen te worden om verdere schade te voorkomen. Om de IT apparatuur en data te herstellen, moeten de herstelprocedures zoals is

omschreven in het DRP worden uitgevoerd. Wanneer de situatie is hersteld, dienen de ondernomen stappen voor herstel te worden gedocumenteerd in de vorm van een logboek.

Er is een advies uitgebracht m.b.t. het nemen van preventieve maatregelen op lange termijn. Om de beveiliging van IT systemen te garanderen, dient een penetratietest uitgevoerd te worden om eventuele kwetsbaarheden in de beveiliging van IT systemen te detecteren. Daarnaast kan verlies van netwerk connectiviteit worden voorkomen door een redundante internetverbinding te implementeren.

Om te voorkomen dat de bedrijfsvoering voor een lange periode wordt onderbroken, kan een alternatieve werklocatie worden ingericht. In het geval van calamiteiten kan op deze locatie worden overgeschakeld, zodat de werking van IT apparatuur (welke bijdraagt aan de continuïteit van de bedrijfsvoering) zo snel mogelijk kan worden hervat.

Vervang verouderde hardware in gebruik om systeem falen te voorkomen. Aangeraden wordt om een secundaire (redundante) ‘core switch’ aan de schaffen en te implementeren in het huidige netwerk. Hierdoor kan verlies van (netwerk) connectiviteit worden voorkomen.

Tot slot is er ook een advies uitgebracht m.b.t. het Disaster Recovery plan. Om te testen of het Disaster Recovery plan effectief inzetbaar is in de praktijk, kan een zogenaamde ‘roll-back’ test worden uitgevoerd. Dit houdt in dat een calamiteit wordt gesimuleerd waarin wordt getest hoe lang het duurt om te herstellen van calamiteiten.

Onderzoek hoe er alsnog een passende oplossing gerealiseerd kan worden wat betreft het herstellen van de configuratie van de SAN opslag omgeving. Helaas was het gedurende het onderzoek niet gelukt een oplossing hiervoor te vinden.

Het regelmatig bijwerken en herzien van het Disaster Recovery plan is essentieel. Wijzigingen zoals bijv. het implementeren van nieuwe apparatuur en het uitbreiden van de risicoanalyse, dienen direct te worden doorgevoerd. Dit draagt uiteindelijk bij aan een effectiever Disaster Recovery plan.

Inhoudsopgave

1. Inleiding

Bijna een derde van de bedrijven geeft toe niet te beschikken over een Disaster Recovery plan door een tekort aan (financiële) middelen, personeel of door gebrek aan besef van de noodzaak hiervan. De bedrijven die wel hebben geïnvesteerd in het ontwikkelen van een Disaster Recovery plan, hebben een goed gevoel over het herstel aan de hand van de strategieën die zij hebben ontwikkeld (Castagna, 2015).

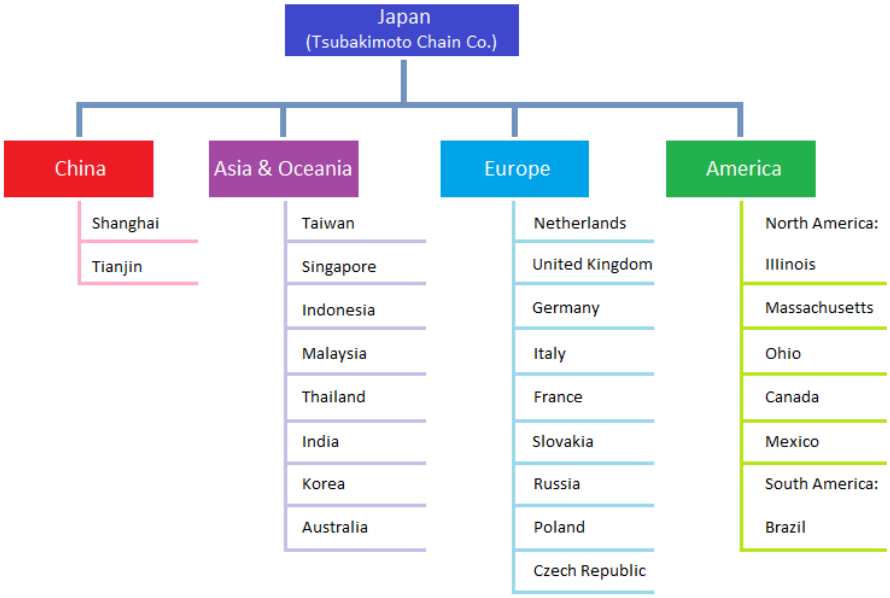
Een Disaster Recovery plan is enkel gericht op het herstel van de functionaliteit van computer systemen/ componenten en andere IT gerelateerde apparatuur na een calamiteit. Het DRP richt zich uitsluitend op calamiteiten op het gebied van IT (NIST, 2010).

Het ontbreken van een *Disaster Recovery plan* (hierna te noemen: DRP) kan desastreuze gevolgen hebben voor organisaties (bijv. financiële schade door onjuist handelen in geval van calamiteiten). Ook voor Tsubakimoto Europe B.V. is het belangrijk te beschikken over een DRP, zodat de verantwoordelijken binnen de organisatie weten welke maatregelen genomen moeten worden om te herstellen van calamiteiten binnen de ICT omgeving.

1.1 Tsubakimoto Europe B.V.

Tsubakimoto Europe B.V. (opgericht in 1972) is een onderdeel van de Tsubakimoto Chain Company en is gevestigd te Dordrecht. De Tsubakimoto Chain Company opereert naast Europa o.a. in de volgende werelddelen: Amerika, Australië en het Midden-Oosten (zie figuur 1). Tsubakimoto Europe B.V. verzorgt de distributie van industriële aandrijfkettingen en aanverwante producten aan distributeurs en *OEM's*.

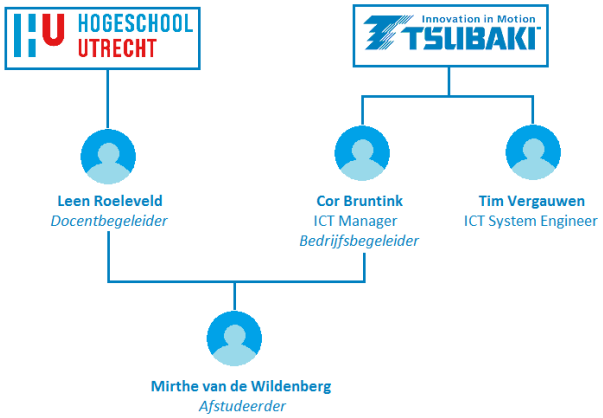
Tsubakimoto Europe B.V. (hierna te noemen: Tsubakimoto) beschikt ook over een moderne werkplaats waar assemblage werkzaamheden worden verricht op de producten voor kant-en-klaar gebruik. De vestiging in Dordrecht is tevens het hoofdkantoor van de Europese tak van de organisatie en telt circa 70 medewerkers. Daarnaast wordt de vestiging te Dordrecht ondersteund door lokale vestigingen in het Verenigd Koninkrijk en Duitsland (Tsubakimoto Europe B.V., 2015).



Figuur 1 **- Tsubakimoto Chain Co.**

1.1.1 Rolverdeling

De afstudeerder zal de afstudeeropdracht uitvoeren binnen de ICT afdeling van Tsubakimoto. Zowel de ICT manager (tevens de bedrijfsbegeleider) als de ICT system engineer zijn beschikbaar voor ondersteuning gedurende de uitvoering van het project (zie figuur 2 voor een overzicht).



***Figuur 2* - Organigram**

1.2 Aanleiding

Hoewel er binnen Tsubakimoto nog geen grote ICT calamiteiten zijn voorgevallen (bijv. een brand in een van de server ruimtes), vindt de directie het wenselijk dat de organisatie op korte termijn beschikt over een DRP. De reden hiervoor is dat Tsubakimoto de intentie heeft om te werken aan een *Business Continuity Plan* (*BCP*), omdat de organisatie zich wilt certificeren volgens de ISO 27001 standaard.

Er zijn binnen Tsubakimoto twee medewerkers verantwoordelijk voor de ICT omgeving. Hiermee beschikt de organisatie niet over de capaciteit om zelf een DRP te realiseren (C. Bruntink, persoonlijke mededeling, 27 september 2015). Om dit project te kunnen uitvoeren, is externe hulp van de afstudeerder ingeschakeld. Omdat Tsubakimoto niet beschikt over een DRP, is het voor hen onduidelijk welke mogelijke calamiteiten zich kunnen voordoen binnen de ICT omgeving en hoe de verantwoordelijken hierbij moeten ingrijpen.

1.3 Projectdoelstellingen

Tsubakimoto wil beschikken over een DRP om minder kwetsbaar te worden voor de risico's op calamiteiten die zich kunnen voordoen binnen de ICT omgeving. Calamiteiten kunnen tijdig worden gesignaleerd wanneer de risico's in kaart worden gebracht waardoor eventuele schade kan worden beperkt en (waar mogelijk) voorkomen, zodat de kritische bedrijfsprocessen en klanten hiervan zo min mogelijk hinder ondervinden. Daarnaast wil Tsubakimoto dat wordt omschreven hoe de verantwoordelijken dienen te handelen in het geval van calamiteiten zodat de bedrijfsvoering zo snel mogelijk hersteld kan worden naar de oorspronkelijke situatie.

1.4 Opdrachtomschrijving en onderzoeksvragen

De opdracht is als volgt geformuleerd; onderzoek welke maatregelen genomen dienen te worden om de risico's op ICT gerelateerde calamiteiten zoveel mogelijk in te perken, en hoe de verantwoordelijken binnen Tsubakimoto dienen in te grijpen wanneer calamiteiten optreden. Vervolgens kunnen op basis van de situatie maatregelen worden genomen om te herstellen van calamiteiten en waar mogelijk preventieve maatregelen worden gedefinieerd om calamiteiten te voorkomen.

1.4.1 Hoofdvraag

"Welke maatregelen zijn noodzakelijk om enerzijds het risico op calamiteiten te minimaliseren en anderzijds adequaat in te grijpen bij calamiteiten?"

1.4.2 Deelvragen

#	Deelvraag	Methode	Functie
1	*Hoe verlopen de kritische bedrijfsprocessen binnen de organisatie?*	(Groeps)gesprekken/ Interviews Analyseren documentatie	Beschrijven
2	*Welke bedrijfskritische systemen/ componenten zijn betrokken bij de kritische bedrijfsprocessen?*	(Groeps)gesprekken/ Interviews Analyseren documentatie	Beschrijven
3	*Welke ICT gerelateerde calamiteiten vormen een risico voor de bedrijfskritische systemen/ componenten?*	Literatuur onderzoek (Groeps)gesprekken/ Interviews	Verklaren
4	*Wat is de impact van een calamiteit, welke zich voordoet binnen de bedrijfskritische systemen/ componenten, op de kritische bedrijfsprocessen?*	(Groeps)gesprekken/ Interviews	Verklaren
5	*Welke maatregelen dienen genomen te worden om het risico op calamiteiten te verminderen en waar mogelijk te voorkomen?*	Literatuur onderzoek (Groeps)gesprekken/ Interviews Observeren	Ontwerpen
6	*Hoe dienen de verantwoordelijken binnen de organisatie te handelen in het geval van een calamiteit?*	Literatuur onderzoek (Groeps)gesprekken/ Interviews	Ontwerpen

Tabel 1 **- Deelvragen**

1.5 Ethische afweging

Er is geen sprake van een directe relatie tussen de problematiek en ethische aspecten (zoals duurzaamheid, wetenschappelijke of sociaal-maatschappelijke aspecten). De uitvoering van het project en de producten dienen echter wel in lijn te zijn met de regelgeving van Tsubakimoto, waarbij de regels met betrekking tot bescherming van bedrijfsgegevens en bedrijfsmiddelen (waaronder apparatuur, producten, machines maar ook bedrijfsprocessen vallen) moeten worden gehandhaafd. Door deze regels op te volgen moet verlies, misbruik of oneigenlijk gebruik van zowel de bedrijfsgegevens als bedrijfsmiddelen worden voorkomen (Tsubakimoto Chain Co, 2008).

1.6 Afbakening

1.6.1 Binnen de scope van het project

- Onderzoeken wat een DRP inhoudt en hoe een risicoanalyse kan worden uitgevoerd;
- Onderzoeken en documenteren wat (het verloop van) de kritische bedrijfsprocessen zijn;
- Onderzoeken en inventariseren welke IT systemen betrokken zijn bij de kritische bedrijfsprocessen;
- Onderzoeken en documenteren welke mogelijke calamiteiten zich kunnen voordoen binnen Tsubakimoto. Hierbij wordt de focus gelegd op de calamiteiten die hun oorzaak vinden in de ICT omgeving, en calamiteiten welke gevolgen kunnen hebben voor de ICT omgeving;
- Onderzoeken welke correctieve en preventieve maatregelen genomen kunnen worden in het geval van een calamiteit. De correctieve en preventieve maatregelen op korte termijn

(preventief: bijv. dat de organisatie op voorhand beschikt over extra apparatuur wanneer een apparaat uitvalt in het geval van een calamiteit) zullen worden opgenomen in het DRP;
- Aan het einde van het project zal een adviesrapport worden opgeleverd waarin preventieve maatregelen op lange termijn (preventieve maatregelen die bijv. veel tijd en geld kosten om te implementeren) worden opgenomen, in de vorm van aanbevelingen;
- Het project zal zich uitsluitend richten op Disaster Recovery planning.

1.6.2 Buiten de scope van het project

- Betrekken van software, applicaties, telefonie, laptops en desktop computers;
- Betrekken van (overige) calamiteiten welke een gevaar vormen voor o.a. het imago, veiligheid en de klanten van de organisatie;
- Aspecten die te maken hebben met Business Continuity planning (BCP) worden buiten beschouwing laten;
- Het contractuele/ wettelijke aspect (wat betreft regelgevingen, standaarden en eisen op het gebied van de ICT binnen organisaties);
- Testen van het DRP.

1.7 Producten

De afstudeeropdracht omvat het verrichten van een descriptief onderzoek. Er is echter ook sprake van een ontwerponderzoek, omdat de omschreven maatregelen in het DRP en aanbevelingen in het adviesrapport bijdragen aan het ontwerp van een nieuwe situatie.

1.7.1 Deelproducten

- Vooronderzoek;
- Procesanalyse;
- IT componenten analyse;
- Risicoanalyse.

1.7.2 Eindproducten

- Het DRP;
- Een adviesrapport;
- De scriptie.

1.8 Leeswijzer

Om de leesbaarheid van de scriptie te bevorderen is gekozen om aan het eind van de inleiding een leeswijzer toe te voegen. Hierin wordt omschreven wat er in de komende hoofdstukken wordt behandeld.

Hoofdstuk twee beschrijft de aanpak en toegepaste projectfasering. Hierin wordt onder meer beschreven hoe de projectfasering in elkaar zit en hoe deze is toegepast. Daarnaast is hierin ook een overzicht opgenomen van de doorgevoerde wijzigingen binnen het project.

In het derde hoofdstuk komt de procesanalyse aan bod, waarin het verloop van de kritische bedrijfsprocessen wordt omschreven.

Hoofdstuk vier omschrijft de IT componentenanalyse, waarin de relatie tussen de kritische bedrijfsprocessen en IT systemen wordt weergegeven in tabelvorm.

In het vijfde hoofdstuk is de risicoanalyse beschreven. Hierin wordt onder andere benadrukt wat de scope is van de risicoanalyse en welke methode en risicocategorieën zijn toegepast.

Hoofdstuk zes omschrijft het Disaster Recovery plan (DRP), waarin de correctieve en preventieve maatregelen zijn uitgewerkt. Daarnaast wordt ook omschreven hoe de verantwoordelijken binnen Tsubakimoto dienen te handelen in het geval van calamiteiten.

In het zevende hoofdstuk worden conclusies en aanbevelingen gegeven. Hierin wordt tevens een antwoord gegeven op de hoofdvraag.

In hoofdstuk acht wordt de evaluatie van de procesgang van het project omschreven.

Tot slot is er een bronnenlijst toegevoegd waarin de gebruikte bronnen en literatuur zijn weergegeven. Na de bronvermelding volgt een overzicht van de gebruikte tabellen en figuren. De cursieve woorden en afkortingen in deze scriptie zijn opgenomen in een woordenlijst.

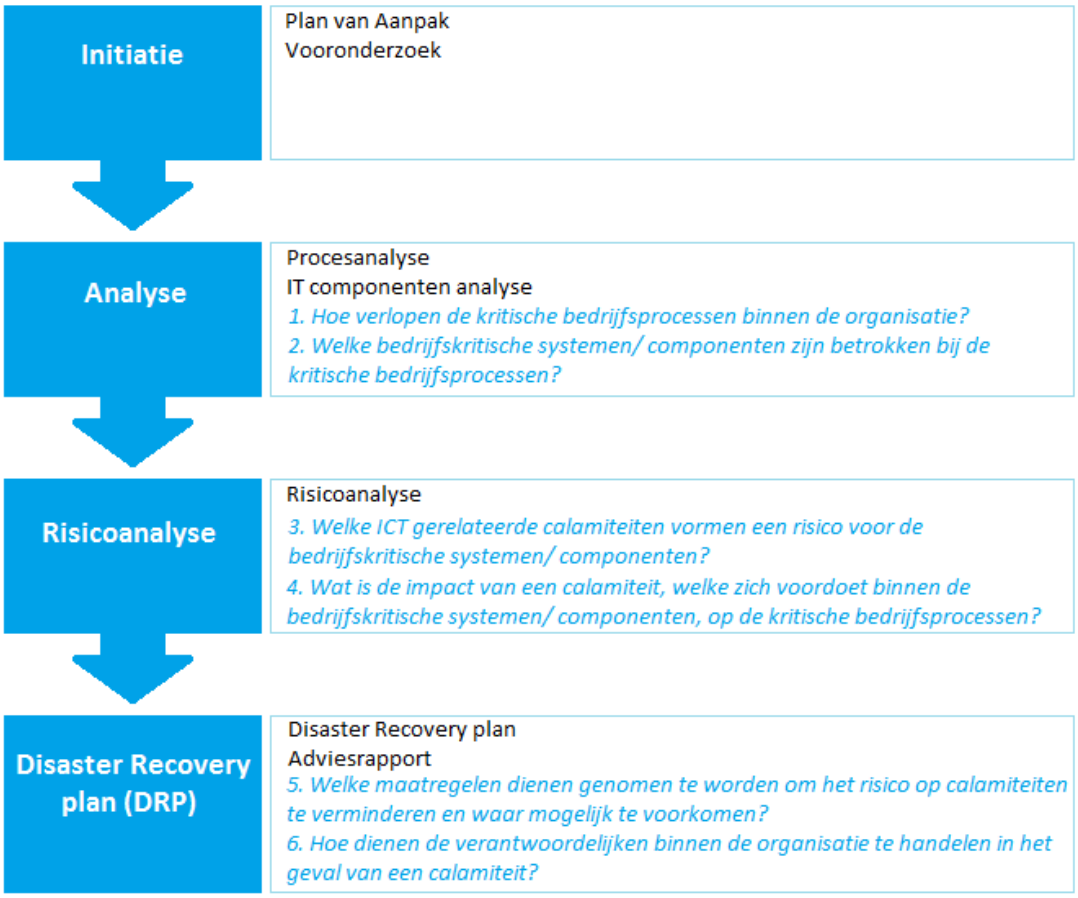
Deze scriptie bevat een aantal bijlagen die apart zijn bijgesloten in het document genaamd "Appendix: Scriptie". In dit bijgesloten document zijn de uitwerkingen van de deelproducten te vinden, het Disaster Recovery plan, het adviesrapport en tot slot de zelfreflectie.

2. Methode en aanpak

Het verloop van het project is ingedeeld volgens de watervalmethode. Er is voor de watervalmethode gekozen omdat het project (net als de watervalmethode) is opgedeeld in een aantal fasen, die achtereenvolgens worden afgewerkt waardoor uiteindelijk het eindproduct -- het DRP -- wordt gerealiseerd (Kennisconsult, 2011).

2.1 Watervalmethode

Figuur 3 toont aan hoe de watervalmethode is toegepast op dit project. Hierbij is ook aangegeven welke deelvraag in welke fase van het project is beantwoord met de bijbehorende 'deliverables'.



Figuur 3 **- Watervalmethode**

2.2 Projectfasering

Het project is verdeeld in een aantal fasen; de initiatie, de analyse (onder te verdelen in de proces analyse en de IT componenten analyse), de risicoanalyse en de Disaster Recovery planning (DRP) fase.

2.2.1 Initiatie

In de initiatie fase is het Plan van Aanpak (PvA) voor het project opgesteld. Daarnaast is gedurende deze fase het vooronderzoek verricht waarin onder meer is onderzocht hoe een risicoanalyse kan worden uitgevoerd, en hoe een DRP tot stand komt.

2.2.2 Analyse (Procesanalyse en IT componenten analyse)

In de analyse fase zijn de kritische bedrijfsprocessen van Tsubakimoto onderzocht en omschreven, d.m.v. het voeren van gesprekken en het bestuderen van documentatie. Volgend op de procesanalyse is een IT componenten analyse (systeeminventarisatie) gemaakt van de IT systemen die zijn betrokken bij deze kritische bedrijfsprocessen, waarin onder meer systeemspecificaties zijn gedocumenteerd. Om een duidelijke relatie te leggen met de kritische bedrijfsprocessen en betrokken IT systemen, is in overleg met de opdrachtgever besloten dit weer te geven in tabelvorm.

2.2.3 Risicoanalyse

In de risicoanalyse fase is onderzocht welke calamiteiten zich mogelijk kunnen voordoen binnen de ICT omgeving van Tsubakimoto. In overleg met de opdrachtgever is besloten alleen de calamiteiten welke een fysieke impact kunnen hebben op de IT systemen en op data mee te nemen in de analyse, waarbij wordt uitgegaan van (totale) systeemuitval en dataverlies. Daarnaast kunnen systeemuitval en dataverlies een hardware gerelateerde, en een niet-hardware gerelateerde oorzaak hebben. Deze aspecten zullen ook mee worden genomen in de scope.

Om de kans en impact te berekenen van deze calamiteiten is gebruik gemaakt van de kwantitatieve methode. De kwantitatieve methode maakt gebruik van metingen en getallen, wat specifieke en meetbare resultaten oplevert (Snedaker, 2014). Daarnaast heeft de kwantitatieve methode het voordeel dat de resultaten exact, herhaalbaar en reproduceerbaar zijn vast te stellen (NIST, 2012).
Omdat er vanuit de organisatie behoefte is aan resultaten die middels berekeningen aantoonbaar kunnen worden onderbouwd, is in overleg met de opdrachtgever besloten om de kwantitatieve methode toe te passen.

2.2.4 Disaster Recovery plan (DRP)

In de Disaster Recovery plan fase is het DRP gerealiseerd. De opbouw van het DRP bevat ten minste de volgende onderwerpen: activering, teamindeling, communicatie, maatregelen voor herstel, een logboek en eventuele bijlagen (Snedaker, 2014). N.a.v. de risicoanalyse zijn de correctieve en preventieve maatregelen beschreven, om het risico op calamiteiten te verminderen en waar mogelijk te voorkomen.

Middels het vormen van herstelteams (bestaande uit stafpersoneel) zijn verantwoordelijkheden gedefinieerd, die verduidelijken hoe de verantwoordelijken binnen Tsubakimoto moeten ingrijpen in het geval van calamiteiten. Hierbij zijn de volgende herstelteams omschreven (overgenomen uit het boek: "*Business Continuity and Disaster Recovery Planning for IT Professionals*" van S. Snedaker), te weten; het 'management team', 'damage assessment team', en 'IT recovery team'. In overleg met de opdrachtgever is het 'functional area team' hieraan toegevoegd. Tot slot zijn in de bijlagen van het DRP onder meer de herstelprocedures opgenomen, waarin staat omschreven hoe de IT systemen in het geval van calamiteiten kunnen worden hersteld.

2.3 Project wijzigingen

Onderstaande tabel toont de wijzigingen die zijn doorgevoerd gedurende de uitvoering van het project:

#	Omschrijving	Goedkeuring door	Datum
1	N.a.v. een overleg met de opdrachtgever is geconstateerd dat deelvraag 4 uit het Plan van Aanpak (*Wat is de impact van de risico's op de bedrijfskritische systemen/ componenten en dus op de primaire bedrijfsprocessen?*) onvolledig is geformuleerd; de nadruk dient te liggen op de impact van een calamiteit. In overleg met zowel de opdrachtgever als de docentbegeleider, is de formulering van deelvraag 4 gewijzigd: "*Wat is de impact van een calamiteit, welke zich voordoet binnen de bedrijfskritische systemen/ componenten, op de primaire bedrijfsprocessen?".*	Cor Bruntink Leen Roeleveld	28-10-2015
2	De formulering van deelvraag 1 uit het Plan van Aanpak (*Hoe verlopen de primaire bedrijfsprocessen binnen de organisatie?*) is gewijzigd in: "*Hoe verlopen de kritische bedrijfsprocessen binnen de organisatie?*". Omdat een aantal van de geïdentificeerde bedrijfsprocessen niet per definitie primaire processen hoeven te zijn, maar wel cruciaal zijn voor de continuïteit van de bedrijfsvoering, is 'primair' daarom vervangen door 'kritisch'. *Hierbij is het woord "primaire" ook vervangen door "kritische" in deelvraag 2 (*Welke bedrijfskritische systemen/ componenten zijn betrokken bij de kritische bedrijfsprocessen?)* en deelvraag 4 (*Wat is de impact van een calamiteit, welke zich voordoet binnen de bedrijfskritische systemen/ componenten, op de primaire bedrijfsprocessen?)*.	Cor Bruntink Leen Roeleveld	27-11-2015

Tabel 2 **- Doorgevoerde project wijzigingen**

3. Kritische bedrijfsprocessen

In dit hoofdstuk wordt het verloop van de kritische bedrijfsprocessen binnen Tsubakimoto omschreven. Onder kritische bedrijfsprocessen wordt het volgende verstaan: wanneer deze processen in het geval van een calamiteit niet uitgevoerd kunnen worden, betekent dit dat Tsubakimoto niet in staat is goederen te factureren en te leveren aan haar klanten, met als mogelijk gevolg klanten en inkomsten te verliezen (E. van Wensveen, persoonlijke mededeling, 25 november 2015).

De onderstaande bedrijfsprocessen zijn gekenmerkt als kritisch:

- 'Control debtors' (controle gegevens van debiteuren);
- 'Creating article record' (aanmaken van een artikel);
- 'Sales quotation' (aanvragen van een offerte);
- 'Sales order' (het plaatsen van een bestelling);
- 'Receipt of goods & warehousing' (ontvangst van goederen);
- 'Order collection, packing & shipment' (verzendklaar maken van goederen);
- 'Margin control & invoicing' (facturatie);
- 'Manual creditor payments' (betaling aan crediteuren);
- 'Backup procedure' (procedures m.b.t. uitvoeren van back-ups);
- 'Restore procedure' (herstellen van IT systemen).

De volgorde van bovenstaande kritische bedrijfsprocessen verloopt als volgt: een offerte wordt omgezet in een order (om een order in te kunnen voeren zijn onder meer de gegevens van een debiteur en artikel benodigd). Vervolgens wordt een order omgezet in een magazijn bon, en worden de goederen geleverd aan de klant. De klant ontvangt hiervan een factuur (E. van Wensveen, persoonlijke mededeling, 25 november 2015).

In overleg met de opdrachtgever zijn de 'Backup procedure' en 'Restore procedure' ook gekenmerkt als kritische bedrijfsprocessen, omdat deze processen de procedures omschrijven wat betreft het uitvoeren van data back-ups en de IT herstelprocedures.

3.1 Verloop kritische bedrijfsprocessen

In dit hoofdstuk wordt het verloop van de kritische bedrijfsprocessen omschreven. Hiermee wordt tevens een antwoord gegeven op de volgende deelvraag: "**Hoe verlopen de kritische bedrijfsprocessen binnen de organisatie?**".

3.1.1 Control debtors

Wanneer een aanvraag wordt ingediend om een debiteur in te voeren of te wijzigen in het systeem, wordt de debiteurensheet ingevuld en geautoriseerd door de sales manager. In geval van een betalingsconditie op rekening, wordt de kredietwaardigheid van de klant gecontroleerd. Na goedkeuring van de sales manager wordt gecontroleerd of de debiteur mogelijk al aanwezig is in het systeem en of er nog betalingen open staan. Indien de debiteur nog niet aanwezig is in het systeem, zal deze a.d.h.v. de gegevens in de debiteurensheet worden ingevoerd door de sales manager (Tsubakimoto Europe B.V., 2014).

3.1.2 Creating article record

Wanneer een verzoek wordt ingediend om een nieuw artikel aan te maken, controleert de afdeling inkoop of het artikel al bestaat in het systeem. In het geval dit een nieuw artikel betreft, wordt het type artikel bepaald alvorens deze wordt aangemaakt in het systeem (Tsubakimoto Europe B.V., 2015).

Tsubakimoto definieert de typen producten als volgt; STP artikelen zijn standaard producten (welke geen assemblage of andere bewerkingen vereisen) en MTP artikelen zijn speciale/ klant specifieke producten (die op maat worden gemaakt voor de klant). Bij het invoeren van een artikel wordt daarnaast een onderscheid gemaakt tussen assemblage en luchtvracht artikelen (producten die per luchtvracht verzonden worden), omdat deze informatie van belang is m.b.t. het invoeren van een order (E. van Wensveen, persoonlijke mededeling, 27 november 2015).

3.1.3 Sales quotation

Een aanvraag voor een offerte wordt ontvangen via fax, telefoon of e-mail. Er wordt een bevestiging van ontvangst verstuurd indien de aanvraag is aanvaard. Indien de aanvraag niet is aanvaard, zal de klant hiervan op de hoogte worden gesteld. Vervolgens wordt gecontroleerd of de aanvraag betrekking heeft op een nieuw MTP artikel, of een bestaand STP artikel.

Een aanvraag wordt in een van de onderstaande categorieën ingedeeld:

With target sales price	Controle of de richtprijs realistisch is o.b.v. de prijs van de leverancier.
Without target sales price	Er wordt een schatting gemaakt van de richtprijs indien deze ontbreekt.
No information	Er is geen relevante informatie aanwezig van de klant of leverancier waardoor er geen prijsinschatting kan worden gemaakt.
Repeat	De aankoopprijs zal worden berekend o.b.v. de ontwikkelingen in de bruto prijzenlijst.

Het formulier om een offerte aan te vragen wordt ingevuld wanneer de juiste categorie is bepaald. Er wordt vervolgens gecontroleerd of het een lokale offerte betreft of dat de offerte moet worden verzonden naar de leverancier:

- Wanneer het een lokale offerte betreft zal de inkoopprijs worden berekend.
- Indien het niet mogelijk is de prijs te berekenen, zal de aanvraag worden verstuurd naar de fabriek in Japan (de leverancier) met het verzoek om hiervoor een offerte samen te stellen. Omdat de productie van de goederen plaatsvindt in de Tsubakimoto fabriek in Japan, worden de meeste producten voor de verkoop hier ingekocht (E. van Wensveen, persoonlijke mededeling, 27 november 2015).

Als de offerte van de leverancier is gecontroleerd op levertijd, hoeveelheid en inkoopprijs zal het artikel worden aangemaakt. Wanneer de offerte is opgesteld en de verkoopprijs is berekend, wordt de offerte na autorisatie naar de klant toegestuurd per e-mail (Tsubakimoto Europe B.V., 2015).

3.1.4 Sales order

Een order kan via fax, telefoon of e-mail worden geplaatst. Vervolgens zal worden bepaald of het een nieuwe order betreft, de order mogelijk al voorkomt in het systeem of dat er een bestaande order moet worden gewijzigd. In geval van een bestaande order wordt gecontroleerd of het mogelijk is om ordergegevens te wijzigen.

Wanneer de order is voltooid wat betreft STP en assemblage artikelen, wordt de orderbevestiging verstuurd naar de klant. De MTP artikelen worden eerst gecontroleerd door de sales afdeling zodra een bevestiging van de leverancier is ontvangen. Daarna zal de orderbevestiging worden verzonden naar de klant (Tsubakimoto Europe B.V., 2015).

3.1.5 Purchase order & confirmation

Met betrekking tot het bestelproces, kan een STP artikel of een MTP artikel worden ingekocht. Wanneer een bestelling wordt geplaatst, wordt deze gecontroleerd op prijs, wisselkoers en leveringsdatum door de afdeling inkoop. Wanneer het bestelproces is voltooid, wordt de bestelling naar de leverancier verzonden. Als een orderbevestiging is ontvangen van de leverancier, controleert de afdeling sales nogmaals of de prijs, levertijd en hoeveelheid overeenkomen met de gegevens van de bestelling (Tsubakimoto Europe B.V., 2015).

3.1.6 Receipt of goods & warehousing

Bij de ontvangst van goederen worden stickers gemaakt o.b.v. het voorontvangst nummer, productcode en locatie. De goederen (die zijn besteld bij de leverancier voor bevoorrading) die zijn ontvangen door het magazijn worden gecontroleerd op eventuele schade alvorens ze worden opgeslagen. Vervolgens wordt de productcode en de locatie waar de goederen worden opgeslagen gescand. Wanneer de goederen zijn opgeslagen op de juiste locatie, wordt de voorraad bijgewerkt in het systeem (Tsubakimoto Europe B.V., 2013).

3.1.7 Order collection, packing & shipment

De warehouse manager creëert magazijn bonnen o.b.v. de orders die verzonden moeten worden. De orders worden verzameld in het magazijn en vervolgens ondertekend. Hierna wordt gecontroleerd of de juiste goederen zijn verzameld. Als de goederen zijn verpakt voor verzending en afgetekend, wordt het totaalgewicht van de zending gecontroleerd. Na goedkeuring zal de magazijn bon op de zending worden geplaatst, en zijn de goederen gereed voor verzending (Tsubakimoto Europe B.V., 2015).

3.1.8 Margin control & invoicing

De sales manager controleert de marge van alle verkooporders a.d.h.v. de informatie op de margelijst, en de informatie op de pakbon. Het verkoopbedrag, de marge en andere kosten worden vermeld op de margelijst. Na autorisatie zal de sales manager de margelijst archiveren. Vervolgens informeert de sales manager de receptie dat de pakbonnen kunnen worden gefactureerd, waarna de originele factuur wordt verstuurd naar de klant (Tsubakimoto Europe B.V., 2013).

3.1.9 Manual creditor payments

De administratie selecteert handmatig facturen die moeten worden betaald aan crediteuren (leveranciers). Vervolgens worden de betalingen in het bank software systeem ingevoerd. De administratie zal dan controleren of de betaling correct is ingevuld. Wanneer deze is goedgekeurd, zal de betaling in het bank software systeem worden geüpload (Tsubakimoto Europe B.V., 2015).

3.1.10 Backup procedure

Een back-up van de servers wordt dagelijks automatisch op de (interne) EMC data back-up server geplaatst. Er is daarnaast ook een extra back-up taak opgenomen voor de e-mail servers (wordt elke laatste zaterdag van de maand uitgevoerd). Van alle bestanden op de data server wordt een back-up gemaakt door Symantec Backup Exec[1]. De back-up van de virtuele servers wordt uitgevoerd door Veeam[2]. Elke vrijdag wordt een *full back-up* uitgevoerd. Op werkdagen (behalve vrijdag) wordt een *incrementele back-up* uitgevoerd. Elke laatste zondag van de maand wordt nogmaals een full back-up uitgevoerd met een retentie van 52 weken. De back-ups worden elke ochtend gecontroleerd en de resultaten worden opgeslagen in een back-up log. Middels *replicatie* worden de back-ups vervolgens dagelijks gesynchroniseerd naar het (externe) datacenter (Tsubakimoto Europe B.V., 2014).

3.1.11 Restore procedure

De IT-afdeling bepaalt wanneer de back-up procedure uitgevoerd dient te worden. Wanneer bestandsherstel vereist is (bijv. als bestanden verloren zijn gegaan), zal Symantec Backup Exec worden gebruikt voor het herstel (vanuit de EMC data back-up server). In het geval van een server storing, zal voor herstel gebruik worden gemaakt van Veeam. Wanneer een herstel proces is voltooid, zal worden gecontroleerd of het herstel proces met succes is verlopen (Tsubakimoto Europe B.V., 2014).

[1] Symantec Backup Exec is een software programma welke in staat is back-ups (en herstel) uit te voeren voor zowel virtuele als fysieke servers (Bron: http://www.symantec.com/en/uk/products/data-backup-software/).

[2] Veeam is een back-up software programma welke back-ups creëert van Windows systemen, zoals laptops en desktops (Bron: http://www.veeam.com/endpoint-backup-free-faq.html).

4. IT systemen en bedrijfsprocessen

Dit hoofdstuk geeft een overzicht van de IT systemen en componenten die de kritische bedrijfsprocessen ondersteunen (tabel 3). Hiermee wordt tevens een antwoord gegeven op de volgende deelvraag: "**Welke bedrijfskritische systemen/ componenten zijn betrokken bij de kritische bedrijfsprocessen?**". Onder elk IT systeem is een korte omschrijving toegevoegd om te verduidelijken welke services worden geraadpleegd door een bepaald bedrijfsproces. Raadpleeg de IT componenten analyse (appendix) voor een volledige omschrijving van de IT systemen.

Business Process	Control Debtors	Creating Article Record	Sales Quotation	Sales Order	Purchase Order & Confirmation	Receipt of Goods & Warehousing	Order collection, packing & shipment	Margin Control & Invoicing	Manual Creditor Payments	Backup Procedure	Restore Procedure
Servers (physical)											
Barracuda Message Archiver 350 - Raadplegen van e-mail berichten (uit archief).			X								
Barracuda Spam Firewall 300 - Verzenden van offerte per e-mail. - Verzenden van orderbevestiging per e-mail.			X	X							
CTXSRV06 - T.b.v. '*thin client*' en 'remote' gebruikers; hiermee wordt tevens de 'Agresso Wholesale' client (een ERP oplossing) gestart, zodat personeel het ERP kan raadplegen.	X	X	X	X	X	X	X	X	X		
DATASRV03 - Raadplegen van ERP gerelateerde documentatie. - Raadplegen proces gerelateerde documentatie.			X	X	X	X	X	X			
DBSRV01 - Bevat de data van de ERP, en omvat onder meer het raadplegen van de ERP database.	X	X	X	X	X	X	X	X	X		
EMCDD01 - Omvat de back-up storage (uitvoeren van back-up en herstel geschiedt vanuit deze server), back-up replicatie naar '*off-site*' back-up storage server.										X	X
LH-SAN01 - Storage server: bevat de layouts van documentatie (zoals orderbevestigingen en offertes) en labels (magazijn bonnen).			X	X		X	X	X	X	X	X
LH-SAN02 - Storage server: bevat de layouts van documentatie (zoals orderbevestigingen en offertes) en labels (magazijn bonnen).			X	X		X	X	X	X	X	X

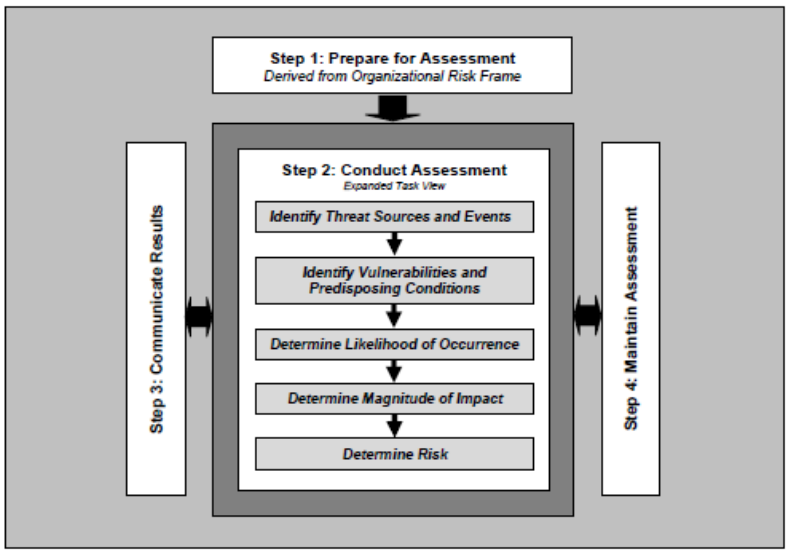
LH-SAN03 - Storage server: bevat de layouts van documentatie (zoals orderbevestigingen en offertes) en labels (magazijn bonnen).			X	X		X	X	X	X	X	X
LH-SAN04 - Storage server: bevat de layouts van documentatie (zoals orderbevestigingen en offertes) en labels (magazijn bonnen).			X	X		X	X	X	X	X	X
VMWSRV01 - T.b.v. de VMware virtuele server omgeving.	X	X	X	X	X	X	X	X	X	X	X
VMWSRV02 - T.b.v. de VMware virtuele server omgeving, en dient als '*failover*' van **VMWSRV01**.	X	X	X	X	X	X	X	X	X	X	X
Servers (VM)											
CTXSRV07 - '*Load balance*' van **CTXSRV06**, t.b.v. 'thin-client' en 'remote' gebruikers.	X	X	X	X	X	X	X	X	X		
DBSRV02 - 'Failover' server van **DBSRV01**.	X	X	X	X	X	X	X	X	X		
DMNSRV02 - Active Directory domein omgeving.			X	X	X	X	X	X			
ELOSRV01 - Raadplegen van documentatie uit (digitaal) archief (m.b.t. documentatie van het ERP).	X		X	X	X		X	X			
EXCSRV02 - T.b.v. de e-mail omgeving (bijv. verzending/ ontvangen van orderbevestigingen, facturen).	X		X	X			X	X			
EXCSRV03 - T.b.v. de e-mail omgeving (bijv. verzending/ ontvangen van orderbevestigingen, facturen).	X		X	X			X	X			
FRONTENDSRV01 - T.b.v. de e-mail omgeving (bijv. verzending/ ontvangen van orderbevestigingen, facturen).	X		X	X			X	X			
PORTALSRV01 - Login portal t.b.v. **CTXSRV06** en **CTXSRV07** Citrix server omgeving.	X	X	X	X	X	X	X	X	X		
RFSRV01 - T.b.v. barcode scannning (middels scannen van barcodes worden RF-signalen verwerkt naar het ERP systeem).						X	X				
SONICSRV01 - Inkoop berichten worden verwerkt naar het ERP systeem (zet excel bestanden om naar XML-berichten welke worden verwerkt door het ERP systeem).					X						
SONICSRV02 - 'Failover' van **SONICSRV01**.					X						
VEEAMSRV01 - Back-up server (t.b.v. het creëren van back-ups en herstellen van servers).										X	X
Switches											
HP ProCurve 4208VL - T.b.v. interne netwerk verbinding.	X	X	X	X	X	X	X	X	X	X	X
HP ProCurve E3500YL-24G-PoE (1) - Netwerk verbinding ('failover') tussen de storage servers (LH-SAN01,LH-SAN02,LH-SAN03,LH-SAN04).	X	X	X	X	X	X	X	X	X	X	X

HP ProCurve E3500YL-24G-PoE (2) - Netwerk verbinding ('failover') tussen de storage servers (LH-SAN01,LH-SAN02,LH-SAN03,LH-SAN04).	X	X	X	X	X	X	X	X	X	X	X
HP ProCurve 2610-12/24 PWR - T.b.v. de RF-omgeving.						X	X				
Motorola RFS6000 (Primary) - T.b.v. de RF-omgeving.						X	X				
Motorola RFS6000 (Secondary) - T.b.v. de RF-omgeving.						X	X				
Router											
Cisco Router C8536 - Internetverkeer (t.b.v. in- en uitgaand e-mail verkeer), downloaden van inkoop- en verzendingsgegevens.			X	X			X				
Firewall											
Juniper Firewall SSG140 - T.b.v. in- en uitgaand e-mail verkeer en VPN verbinding (remote toegang middels VPN wordt geautoriseerd door de Firewall).			X	X			X				

Tabel 3 **- Relatie IT systemen/ componenten en kritische bedrijfsprocessen**

5. Risicoanalyse

De uitvoering van de risicoanalyse is gebaseerd op de aanpak zoals is omschreven in de standaard van het National Institute of Standards and Technology (NIST): *Guide for Conducting Risk Assessments* (Special Publication 800-30). Figuur 4 illustreert deze aanpak:



Figuur 4 **- Risk Assessment Process. Overgenomen uit NIST Special Publication 800-30, Rev. 1. *Guide for Conducting Risk Assessments* (p. 24) door NIST, 2012.**

Deze standaard is gekozen omdat ze specifiek is gericht op de uitvoering van een risicobeoordeling op het gebied van de IT. Gezien de beperkte tijd, is in overleg met de opdrachtgever besloten deze aanpak gedeeltelijk over te nemen. De volgende aspecten zijn uit deze aanpak toegepast:

1. Prepare for assessment Bepalen van het doel, de scope, methode, aannames en beperkingen m.b.t. het uitvoeren van de risicoanalyse (NIST, 2012). Het definiëren van aannames en beperkingen zijn niet meegenomen in dit project.

2. Conduct assessment Identificeren welke mogelijke calamiteiten zich zoal kunnen voordoen. Hierbij is tevens omschreven wat de kans, impact en kwetsbaarheden zijn m.b.t. het risico op calamiteiten (NIST, 2012). M.b.t. dit project zijn kwetsbaarheden (‘vulnerabilities’) niet meegenomen, maar zijn in plaats hiervan de huidige ‘*bottlenecks*’ binnen Tsubakimoto omschreven.

3. Communicate results Communiceren en presenteren van de resultaten van de risicoanalyse, bijv. in de vorm van documentatie (NIST, 2012). In de appendix is deze documentatie te vinden (‘Risk analysis’).

4. Maintain assessment Omvat het onderhouden en bijwerken van de risicoanalyse wanneer wijzigingen worden doorgevoerd binnen de organisatie (NIST, 2012). Dit onderdeel is niet meegenomen in dit project.

5.1 Scope risicoanalyse

Er zijn tal van calamiteiten die mogelijk kunnen optreden binnen de ICT omgeving van Tsubakimoto. Om voorafgaand aan de risicoanalyse duidelijk af te bakenen waar de focus ligt, is in overleg met de opdrachtgever besloten dat de risicoanalyse zich beperkt tot de calamiteiten die een fysieke impact hebben op IT systemen, componenten en data. Uiteraard kan er ook sprake zijn van calamiteiten die geen fysieke impact hebben op de IT systemen en data. Deze calamiteiten worden echter niet meegenomen in de risicobeoordeling, omdat de opdrachtgever zich wilt richten op de "ergst mogelijke situatie"; waarbij is uitgegaan van (totale) uitval van IT systemen en dataverlies.

De scope is als volgt gedefinieerd:

- Calamiteiten welke een fysieke impact hebben op de IT systemen, componenten en data worden meegenomen in de risicobeoordeling. Hierbij is uitgegaan van (totale) uitval van IT systemen en dataverlies;
- Er wordt van uitgegaan dat men op de huidige locatie kan blijven doorwerken;
- De calamiteiten in de risicobeoordeling zijn in de volgende categorieën ingedeeld: 'Natural & Environmental', 'Criminal', 'Personnel' en 'Technological';
- De kwantitatieve methode is toegepast om kans, impact en risico op calamiteiten te berekenen;
- Laptops, telefonie, applicaties en software vallen buiten de scope van dit project, en zullen m.b.t. de risicoanalyse dan ook buiten de scope vallen.

5.2 Risicocategorieën

Middels het vaststellen van categorieën kunnen risico's overzichtelijker worden georganiseerd en beheerd (Mitre, z.d.). In overleg met de opdrachtgever zijn vier verschillende categorieën gedefinieerd, te weten: 'Natural & Environmental', 'Criminal', 'Personnel' en 'Technological'.

5.2.1 Natural & Environmental

Onder deze categorie vallen calamiteiten zoals brand en waterschade. In overleg met de opdrachtgever is besloten dergelijke calamiteiten op te nemen in de risicobeoordeling, omdat deze calamiteiten fysieke gevolgen kunnen hebben voor de IT systemen, componenten en data (en dus ook op de continuïteit van de kritische bedrijfsprocessen).

5.2.2 Criminal

Calamiteiten zoals malware/ virusaanvallen en inbraak vallen onder deze categorie. Virusaanvallen kunnen een fysieke impact hebben op bedrijfskritische gegevens; data kan worden gewijzigd of zelfs worden verwijderd. Daarnaast is het ook mogelijk dat er wordt ingebroken door derden, met alle gevolgen van dien (bijv. vernieling van IT apparatuur of diefstal van IT apparatuur en gegevens). Calamiteiten zoals *phishing* en *hacking* vallen bijvoorbeeld ook onder deze categorie, maar omdat deze calamiteiten geen fysieke impact hebben op bedrijfskritische gegevens worden dergelijke calamiteiten niet opgenomen in de risicobeoordeling.

5.2.3 Personnel

Onder deze categorie vallen calamiteiten die veroorzaakt kunnen worden door onopzettelijk handelen van het personeel. Hieronder vallen calamiteiten zoals het per ongeluk verwijderen of aanpassen van data. Er zijn echter ook calamiteiten die kunnen optreden door opzettelijk toedoen van personeel, zoals het opzettelijk verwijderen of zelfs vernietigen van IT systemen en data.

In overleg met de opdrachtgever is besloten alleen de calamiteiten die veroorzaakt kunnen worden door onopzettelijk handelen van personeel op te nemen in de risicobeoordeling, omdat deze calamiteiten op regelmatige basis voorkomen binnen Tsubakimoto. Omdat calamiteiten door opzettelijk handelen van personeel zich ook kunnen voordoen, maar tot op heden nooit zijn voorgekomen binnen Tsubakimoto, is in overleg besloten deze calamiteit daarom niet mee te nemen in de risicobeoordeling.

5.2.4 Technological

Calamiteiten die ontstaan in de ICT omgeving, zoals een systeemcrash of hardware falen, vallen onder deze categorie. Deze calamiteiten kunnen onder meer leiden tot dataverlies en verlies van netwerk connectiviteit.

Omdat in deze risicoanalyse wordt uitgegaan van totale uitval, is in overleg met de opdrachtgever besloten deze drie aspecten mee te nemen in de risicobeoordeling: dataverlies, verlies van IT systemen/ componenten en verlies van netwerk connectiviteit.

5.3 Risicobeoordeling

Om de gegevens van de risicobeoordeling overzichtelijk te inventariseren, is met goedkeuring van de opdrachtgever ervoor gekozen de resultaten in tabelvorm te presenteren. De opbouw van tabel 4 (“Inventarisatie calamiteiten”) en tabel 5 (“Effectenbeoordeling”) is gedeeltelijk gebaseerd op onderstaande afbeelding (figuur 5):

Table 4.4 Risk Assessment Table

Item No	Threat Name	Threat Source	Vulnerability Rating	Likelihood Rating	Existing Controls	Impact Rating	Overall Risk Rating
001	Fire	Internal					
002		External					
003	Flood	Internal					

Figuur 5 **- Risk Assessment Table. Overgenomen uit *Business Continuity and Disaster Recovery Planning for IT Professionals* (p. 201) door Snedaker, S., 2014.**

Opbouw tabel 4:

Threat Area	Potential threat	Current bottlenecks

De ‘Threat Area’ kolom komt overeen met de ‘Threat Name’ kolom. In deze kolom zijn de geïdentificeerde calamiteiten genoemd.

De ‘Potential threat’ kolom komt overeen met de ‘Threat Source’ kolom. In deze kolom is een omschrijving weergegeven van de bijbehorende calamiteit.

De ‘Current bottlenecks’ kolom komt overeen met de ‘Vulnerability Rating’ kolom. In deze kolom zijn de bestaande ‘bottlenecks’ die binnen Tsubakimoto aanwezig zijn (per calamiteit) in kaart gebracht.

Opbouw tabel 5:

Threat Area	Potential threat	Probability (annually)	Impact (costs per incident)	Risk (total cost)

De 'Probability (annually)' kolom komt overeen met de 'Likelihood Rating' kolom. Hierbij is de kans gebaseerd op het aantal calamiteiten op jaarbasis.

De 'Impact (costs per incident)' kolom komt overeen met de 'Impact Rating' kolom. Hierbij is de impact gebaseerd op het aantal kosten per calamiteit; uitgedrukt in kosten aan verloren manuren en de kosten van IT apparatuur.

De 'Risk (total cost)' kolom komt overeen met de 'Overall Risk Rating' kolom. Het totaal aantal kosten (de risicofactor) is berekend met de volgende formule: Risico = kans x impact. Raadpleeg bijlage B voor de berekeningen en verantwoording van de resultaten.

5.3.1 Dreigingsanalyse

In de onderstaande tabel (tabel 4) zijn de calamiteiten en huidige 'bottlenecks' geïnventariseerd. Hiermee wordt tevens een antwoord gegeven op de volgende deelvraag: "**Welke ICT gerelateerde calamiteiten vormen een risico voor de bedrijfskritische systemen/ componenten?**".

Threat Area	Potential threat	Current bottlenecks
Natural & Environmental		
Fire	*IT equipment (and therefore, data) may be lost in case of a fire.*	• There is currently no replacement IT equipment available (when crucial IT systems are lost in case of a fire, and no replacement systems are available, it may cause a major disruption and therefore, financial losses for the organization).
	Collateral damage: smoke/ soot damage which might cause damaged or loss of IT equipment (and therefore, data).	• There is currently no replacement IT equipment available.
Water damage	*Leakage: heavy rain or leaking pipes, frost/thaw might cause damaged or loss of IT equipment (and therefore, data).*	• No periodically controls to check if there are no damaged pipes or weak spots in roofs; • There is currently no replacement IT equipment available.
Power outage	*Electrical storms or a short circuit in power supply may cause a power outage.*	
Criminal		
Malware/ virus attacks	*Malware or viruses are capable of data deletion, destruction or manipulation.*	• No penetration tests performed.

Burglary	*Vandalism: damaged or loss of IT equipment (and therefore, data).*	• The server racks in the server room are not locked (if a third party breaks into one of the server rooms, IT equipment might be damaged); • There is currently no replacement IT equipment available.
	Theft: loss of IT equipment (and therefore, data).	• The server racks in the server room are not locked (if a third party breaks into one of the server rooms, IT equipment might be stolen); • There is currently no replacement IT equipment available.
Personnel		
Accidental actions	*Altering, deleting, destroying data (accidental deletion of data or accidental altering of data which also might cause data loss).*	• Configuration mistakes might give personnel privileged access.
Technological		
Hardware issues/ failure	*Loss of data.*	• A backup job might fail, which causes data loss.
	Loss of network connectivity: (i.e. no access to the internet or e-mail)	• Old hardware is still in use, which might cause equipment to malfunction; • No failover regarding internet connectivity implemented; • Core switch of the network is not redundant.
	Loss of IT equipment: (i.e. a defect in the hard disk which causes the system to crash).	• Old hardware is still in use, which might cause equipment to malfunction; • There is currently no replacement IT equipment available.
Vendor failure	*Loss of IT equipment (i.e. due to a fire at the vendor's location) – the (secondary) backup server is hosted at an off-site location.*	• There is currently no replacement IT equipment available (regarding a backup server).

Tabel 4 - Inventarisatie calamiteiten

5.3.2 Calamiteiten: kans en impact

In dit hoofdstuk is een schatting gemaakt van de kans (op jaarbasis) en de impact (uitgedrukt in hardware kosten en kosten aan verloren manuren) wanneer een calamiteit zich voordoet. Hiermee wordt tevens antwoord gegeven op de volgende deelvraag: "**Wat is de impact van een calamiteit, welke zich voordoet binnen de bedrijfskritische systemen/ componenten, op de kritische bedrijfsprocessen?**".

Threat Area	Potential threat	Probability (annually)	Impact (costs per incident)	Risk (total cost)
	Natural & Environmental			
Fire	*IT equipment (and therefore, data) may be lost in case of a fire.*	0,0001	€ 180.000,00	€ 18,00
	Collateral damage: smoke/ soot damage which might cause damaged or loss of IT equipment (and therefore, data).	0,0001	€ 180.000,00	€ 18,00
Water damage	*Leakage: heavy rain or leaking pipes, frost/thaw might cause damaged or loss of IT equipment (and therefore, data).*	0,001	€ 180.000,00	€ 180,00
Power outage	*Electrical storms or a short circuit in power supply may cause a power outage.*	0,08	€ 1250,00	€ 100,00
	Criminal			
Malware/ virus attacks	*Malware or viruses are capable of data deletion, destruction or manipulation.*	2	€ 5000,00	€ 10.000,00
Burglary	*Vandalism: damaged or loss of IT equipment (and therefore, data).*	0,2	€ 180.000,00	€ 36.000,00
	Theft: loss of IT equipment (and therefore, data).	0,2	€ 180.000,00	€ 36.000,00
	Personnel			
Accidental actions	*Altering, deleting, destroying data (accidental deletion of data or accidental altering of data which also might cause data loss).*	10	€ 6,25	€ 62,50
	Technological			
Hardware issues/ failure	*Loss of data.*	0,2	€ 50,00	€ 10,00
	Loss of network connectivity: (i.e. no access to the internet or e-mail)	2	€ 5000,00	€ 10.000,00
	Loss of IT equipment: (i.e. a defect in the hard disk which causes the system to crash).	0,2	€ 125.000,00	€ 25.000,00

Vendor failure	*Loss of IT equipment (i.e. due to a fire at the vendor's location) – the secondary backup server is hosted at an off-site location.*	0,0001	€ 6.000,00	€ 0,60

Tabel 5 **- Effectenbeoordeling**

6. Disaster Recovery planning

In dit hoofdstuk zal de toegepaste opbouw van het DRP voor Tsubakimoto worden omschreven. De inhoud van het DRP is gebaseerd op de aanpak die is omschreven in het boek: "*Business Continuity and Disaster Recovery Planning for IT Professionals*" van S. Snedaker.

Deze aanpak bestaat uit de volgende elementen die opgenomen dienen te worden in het DRP: een omschrijving van de activatie van het DRP (onder welke omstandigheden dient het DRP te worden geraadpleegd), het definiëren van herstel teams (waarin de rollen en verantwoordelijkheden van stafpersoneel worden omschreven), communicatie, maatregelen voor herstel (het nemen van correctieve en preventieve maatregelen om het risico op calamiteiten te verminderen en mogelijk te voorkomen) en een logboek met eventuele bijlagen (Snedaker, 2014).

Activering
Er dient een procedure omschreven te worden waarin onder meer wordt gedefinieerd wanneer het DRP geactiveerd moet worden. Het activeren van het Disaster Recovery plan omvat onder andere aanmelding van het incident, beoordeling van het incident en implementatie van herstelprocedures. Het DRP dient op een periodieke basis te worden herzien, om ervoor te zorgen dat het plan actueel en relevant blijft. Bijv. als operatieve of technologische wijzigingen zijn toegepast (zoals het wijzigen van locatie), moeten deze wijzigingen ook in het DRP worden doorgevoerd (Snedaker, 2014).

Teamindeling
Binnen de organisatie is het inschakelen van stafpersoneel noodzakelijk voor activering, implementatie en onderhoud van het DRP. Hiervoor dienen teams gevormd te worden om voor, tijdens en na een verstoring verschillende activiteiten en procedures uit te kunnen voeren. Een goede teambeschrijving omvat onder meer de volgende onderdelen: posities, contact informatie en verantwoordelijkheden (Snedaker, 2014).

Communicatie
Wanneer calamiteiten optreden binnen de organisatie, moet er ook worden omschreven hoe een gesignaleerde calamiteit wordt gecommuniceerd naar de herstel teams, om stafpersoneel op de hoogte te stellen van de situatie (Snedaker, 2014).

Maatregelen voor herstel
Het nemen van maatregelen vloeit voort uit de risico's die zijn geïdentificeerd gedurende de risicoanalyse. Deze maatregelen zijn de onmiddellijke reactie op een calamiteit en omschrijven hoe het risico op calamiteiten kan worden gereduceerd en mogelijk voorkomen (Snedaker, 2014).

Logboek en bijlagen
Een logboek omvat een beschrijving van de gebeurtenissen die hebben geleid tot een calamiteit. Middels het bijhouden van een logboek kunnen de gebeurtenissen op papier worden gezet zodat is vastgelegd welke acties zijn ondernomen om te herstellen na calamiteiten. Andere relevante documentatie (bijv. een systeeminventarisatie, systeemconfiguraties en systeem herstelprocedures) kan worden opgenomen in de bijlage van het DRP (Snedaker, 2014).

6.1 Maatregelen

In dit hoofdstuk zijn de correctieve en preventieve maatregelen omschreven die betrekking hebben op de volgende calamiteiten, te weten: brand, waterschade, stroomuitval, malware/ virusaanval, inbraak, incidenteel handelen, hardware falen en falen van de leverancier. Hiermee wordt tevens een antwoord gegeven op de volgende deelvraag: "**Welke maatregelen dienen genomen te worden om het risico op calamiteiten te verminderen en waar mogelijk te voorkomen?**".

Eventuele maatregelen die al zijn geïmplementeerd binnen Tsubakimoto worden ook omschreven. De omschrijving van de correctieve en preventieve maatregelen is terug te vinden in het Disaster Recovery plan (appendix).

Brand

De volgende maatregelen zijn reeds binnen Tsubakimoto geïmplementeerd om het risico op een brand te verminderen: binnen de faciliteit is een brandalarm geïmplementeerd, en er wordt twee keer per jaar een brandoefening uitgevoerd (zodat het personeel bewust is van het evacuatieproces). Een keer per jaar wordt door de brandweer een controle uitgevoerd binnen de faciliteit om de brandveiligheid te garanderen. Daarnaast beschikt de faciliteit over brandwerende muren (T. Vergauwen, persoonlijke mededeling, 23 november 2015).

Om het risico op een brand te reduceren, dienen IT systemen en componenten regelmatig onderhouden en gecontroleerd te worden om eventuele defecten tijdig te kunnen signaleren en te herstellen (bijv. oververhitting van de voeding in een IT systeem kan een brand veroorzaken) (Fire prevention, z.d.). Door een rookdetectie systeem te implementeren in de server ruimte en brandbestrijdingsmiddelen te onderhouden (zoals brandblussers), kan een brand in een vroeg stadium worden verholpen waardoor de schade aan IT systemen en componenten kan worden beperkt (Brakel Atmos, z.d.).

De onderstaande correctieve maatregelen verminderen het risico (en de impact) op een brand:

- Controleer regelmatig de IT systemen en componenten op eventuele defecten;
- Implementeer een rookdetectie systeem binnen de faciliteit (zoals de server ruimte);
- Onderhouden van brandbestrijdingsmiddelen.

Waterschade

Controleer het dak en de waterleidingen regelmatig op mogelijke lekkages of scheuren, zodat het risico op waterschade wordt verminderd (Hiscox, z.d.). In de wintermaanden dient het dak vrij gemaakt te worden van sneeuw- en ijsvorming om lekkages te voorkomen (Axis Insurance, z.d.).

De onderstaande correctieve maatregelen verminderen het risico op waterschade:

- Controleer regelmatig het dak en de waterleidingen op mogelijke lekkage/ beschadigingen.

De onderstaande preventieve maatregel kan waterschade voorkomen:

- Maak het dak regelmatig vrij van sneeuw- en ijsvorming.

Stroomuitval
De volgende maatregelen zijn reeds binnen Tsubakimoto geïmplementeerd om het risico op een stroomstoring te verminderen: binnen de faciliteit is een noodstroomvoorziening aanwezig, zodat de IT systemen nog kunnen functioneren voor een beperkte tijd. Op het dak van de faciliteit zijn een aantal bliksemafleiders geïmplementeerd, om een stroomstoring door blikseminslag te voorkomen (T. Vergauwen, persoonlijke mededeling, 23 november 2015).

Beschadiging van bijv. de kabelisolatie kan kortsluiting veroorzaken binnen de faciliteit met mogelijk stroomuitval tot gevolg. Daarnaast is IT apparatuur vatbaar voor stof, wat tevens een stroomstoring kan veroorzaken doordat componenten sneller oververhit kunnen raken. Door de IT apparatuur regelmatig te reinigen van stof en apparatuur te vervangen in geval van eventuele schade, kan een stroomstoring worden voorkomen (ElektricienNu, z.d.).

Onderstaande preventieve maatregelen voorkomen het risico op een stroomstoring:
- Regelmatig controleren, onderhouden en tijdig vervangen van bekabeling, IT systemen en componenten.

Malware/ virusaanval
De volgende maatregelen zijn reeds binnen Tsubakimoto geïmplementeerd om het risico op een virusaanval verminderen: de IT systemen worden regelmatig gescand door een antivirus programma om potentiële virusaanvallen tijdig te detecteren. Hierbij worden ook alle besturingssystemen en het antivirus software programma regelmatig geüpdatet. In het geval van een virusaanval wordt de geïnfecteerde locatie op een IT systeem geïsoleerd om verspreiding te voorkomen, zodat het virus kan worden verwijderd. Tot slot is binnen de ICT omgeving een firewall geïmplementeerd om het risico op een virusaanval te reduceren (T. Vergauwen, persoonlijke mededeling, 23 november 2015).

Om het risico op een virusaanval te verminderen, kan additionele antivirus software worden geïnstalleerd. Door verschillende antivirus programma's of *tools* te gebruiken, kan een groter aantal verschillende typen virussen worden gedetecteerd, waardoor de IT systemen beter beveiligd zijn tegen een breed scala aan potentiële virusaanvallen. Een andere maatregel om het risico op een malware/ virusaanval te verminderen, is door meer bewustzijn te creëren onder het personeel over de verschillende wijzen waarop virussen zich kunnen verspreiden. Om dataverlies te voorkomen in geval van een virusaanval, dient er regelmatiger -- d.w.z. een keer per uur -- een back-up uitgevoerd te worden.

De onderstaande correctieve maatregelen verminderen het risico op een virusaanval:
- Installeer additionele antivirus producten die een breder scala aan virussen kunnen detecteren;
- Creëer bewustzijn onder het personeel over de verspreiding van virussen.

Inbraak
De volgende maatregelen zijn reeds binnen Tsubakimoto geïmplementeerd om het risico op een inbraak verminderen: buiten de faciliteit is bewegingsdetectie verlichting geïmplementeerd. Daarnaast heeft de faciliteit beschikking over een alarm- en camerasysteem. Beide server ruimtes binnen de faciliteit zijn voorzien van een deurslot (T. Vergauwen, persoonlijke mededeling, 23 november 2015).

Hoewel beide server ruimtes zijn afgesloten, kan het ook noodzakelijk zijn de server stellingen te voorzien van een slot. Hierdoor wordt het risico op diefstal en vandalisme van IT systemen en componenten verminderd. Daarnaast dient onbeheerde toegang tot de server ruimtes vermeden te worden om het risico op diefstal en/ of vandalisme te voorkomen. Door vervangende IT apparatuur aan te schaffen en regelmatig een back-up te maken van data, kan verlies van IT apparatuur en dataverlies door diefstal en vandalisme worden voorkomen. Daarnaast kan diefstal van vervangende apparatuur en andere onderdelen ook worden voorkomen door deze apparatuur op te slaan in een kluis.

De onderstaande correctieve maatregel kan het risico op diefstal/ vandalisme (en dus beschadiging of verlies van IT systemen/ componenten) verminderen:

- Voorzie de server stellingen van een slot.

De onderstaande preventieve maatregelen kunnen inbraak (en dus diefstal/ vandalisme) voorkomen:

- Vermijd onbeheerde toegang tot de server ruimtes;
- Voorkom dataverlies door regelmatiger back-ups uit te voeren (een keer per uur).
- Voorkom verlies van IT apparatuur door vervangende apparatuur (zoals servers en switches) aan te schaffen;
- Sla vervangende apparatuur en additionele onderdelen op in een kluis.

Incidenteel handelen

Er is een mogelijkheid dat het personeel per ongeluk data zou kunnen wijzigen of verwijderen. Momenteel wordt binnen Tsubakimoto eenmaal per dag een back-up gemaakt van alle data. Het kan echter voorkomen dat een back-up taak faalt, waardoor dataverlies kan optreden (T. Vergauwen, persoonlijke mededeling, 23 november 2015). Om dataverlies te voorkomen, dient er regelmatiger -- d.w.z. een keer per uur -- een back-up uitgevoerd te worden.

De onderstaande preventieve maatregel kan dataverlies voorkomen:

- Regelmatiger uitvoeren van back-ups (een keer per uur).

Hardware falen

De volgende maatregelen zijn reeds binnen Tsubakimoto geïmplementeerd om het risico op hardware falen te verminderen: alle fysieke servers beschikken over een redundante voeding, wat het risico op uitval van een systeem verminderd. De secundaire (redundante) voeding neemt de andere voeding over wanneer deze is uitgevallen, waardoor het IT systeem kan blijven functioneren. Om het risico op dataverlies zoveel mogelijk in te perken, wordt dagelijks een back-up uitgevoerd. De secundaire back-up server bevindt zich binnen een externe locatie; in het geval wanneer de back-up server binnen Tsubakimoto uitvalt, wordt dataverlies voorkomen doordat de data ook op de externe back-up server is opgeslagen. Tot slot zijn de server ruimtes voldoende geventileerd, waardoor oververhitting van IT systemen (en dus uitval van IT apparatuur) kan worden voorkomen (T. Vergauwen, persoonlijke mededeling, 23 november 2015).

Om het risico op hardware falen en verlies van netwerk connectiviteit te verminderen, dient oude (afgeschreven) apparatuur in gebruik te worden vervangen. Alle hardware en componenten dienen daarnaast regelmatig te worden onderhouden om het risico op hardware falen te verminderen zodat eventuele defecten tijdig kunnen worden gesignaleerd en hersteld. Door vervangende IT apparatuur aan te schaffen en regelmatig een back-up te maken van data, kan verlies van IT apparatuur en dataverlies worden voorkomen (Harbaugh, 2009).

De onderstaande correctieve maatregelen verminderen het risico op systeemuitval:
- Vervang oude (afgeschreven) hardware in gebruik;
- Regelmatig onderhouden van de hardware zodat potentiële defecten tijdig kunnen worden gesignaleerd en hersteld.

De onderstaande preventieve maatregelen kunnen dataverlies en systeemuitval voorkomen:
- Regelmatiger uitvoeren van back-ups (een keer per uur);
- Schaf vervangende IT apparatuur aan om, zodat IT systemen en componenten direct kunnen worden vervangen in het geval van systeemuitval.

Falen van de leverancier
De tweede (redundante) back-up server van Tsubakimoto is gelokaliseerd in een extern datacenter welke wordt beheerd door een derde partij. Ook binnen deze externe faciliteit is het mogelijk dat er calamiteiten optreden wat kan leiden tot systeemverlies (bijv. door het uitbreken van een brand is de secundaire back-up server verloren gegaan). Om systeemverlies te voorkomen, dient een vervangende back-up server te worden aangeschaft zodat deze direct kan worden vervangen.

De onderstaande preventieve maatregelen kan systeemuitval voorkomen:
- Aanschaffen van een vervangende (tweede) back-up server.

6.2 Disaster Recovery teams

In dit hoofdstuk wordt de handelswijze omschreven die de verantwoordelijken (d.w.z. stafpersoneel) binnen Tsubakimoto in het geval van een calamiteit dienen uit te voeren. Hiermee wordt tevens een antwoord gegeven op de volgende deelvraag: "**Hoe dienen de verantwoordelijken binnen de organisatie te handelen in het geval van een calamiteit?**".

In het geval van calamiteiten is een groep mensen benodigd om bepaalde beslissingen te nemen (bijv. mensen die de situatie beoordelen, en beslissingen nemen om het DRP -- of delen daarvan -- te activeren). Daarom is het belangrijk om zogenaamde herstelteams samen te stellen. Deze herstelteams bestaan uit gedefinieerde rollen en verantwoordelijkheden per team, die verduidelijken hoe de verantwoordelijken (d.w.z. stafpersoneel) dienen te handelen in het geval van een calamiteit. Hierbij beschikt elk team over bepaalde verantwoordelijkheden (Snedaker, 2014).

In overleg met de opdrachtgever zijn de volgende herstelteams samengesteld, te weten: het ‘management team’, het ‘damage assessment team’, het ‘IT recovery team’ en het ‘functional area team’. De benaming van deze herstelteams zijn overgenomen uit het boek: “*Business Continuity and Disaster Recovery Planning for IT Professionals*” van S. Snedaker (2014). Een uitgebreide omschrijving van de herstelteams, rollen en verantwoordelijkheden is terug te vinden in het Disaster Recovery plan (appendix).

6.2.1 Management team

Het ‘management team’ is verantwoordelijk voor het maken van bedrijfsgerelateerde beslissingen. In het geval van calamiteiten is het ‘management team’ verantwoordelijk voor het goedkeuren van investeringen (op het gebied van bijv. vervangende IT apparatuur), en dient het team erop toe te zien dat de verantwoordelijken binnen de organisatie de rollen en verantwoordelijkheden uitoefenen zoals is omschreven in het DRP (Snedaker, 2014).

6.2.2 Damage assessment team

In het geval van calamiteiten bepaalt het ‘damage assessment team’ of het Disaster Recovery plan geraadpleegd dient te worden, aan de hand van de criteria die zijn omschreven in het DRP. In overleg met de opdrachtgever zijn volgende criteria gedefinieerd: beschadiging of verlies van IT systemen, beschadiging of verlies van data en verlies van uitbestede diensten. Het ‘damage assessment team’ is ook verantwoordelijk voor het in kaart brengen van eventuele schade aan IT systemen en data (Snedaker, 2014).

In overleg met de opdrachtgever zijn de volgende verantwoordelijkheden toegevoegd: wanneer extra ondersteuning benodigd is voor herstel na een calamiteit, is het ‘damage assessment team’ verantwoordelijk voor het inhuren van extern personeel. Daarnaast dient het ‘damage assessment team’ contact op te nemen met leveranciers wanneer vervangende IT apparatuur aangeschaft moet worden. Nadat de eventuele schade is vastgesteld, dient het ‘damage assessment team’ de te verwachte kosten (voor reparatie, vervanging van apparatuur) te rapporteren aan het ‘management team’.

6.2.3 IT recovery team

Het ‘IT recovery team’ komt nauw overeen met het ‘damage assessment team’, maar het ‘IT recovery team’ heeft echter een aantal andere verantwoordelijkheden dan het ‘damage assesment team’. Het ‘IT recovery team’ is onder meer verantwoordelijk voor het vaststellen van eventuele schade aan IT systemen, componenten en data in het geval van calamiteiten. Daarnaast dient het ‘IT recovery team’ -- afhankelijk van de situatie -- maatregelen te nemen om verdere schade te voorkomen (bijv. een virusaanval isoleren om beschadiging van bestanden te minimaliseren). Er dient ook voldoende vervangende IT (rand)apparatuur beschikbaar te zijn in het geval systemen en componenten vervangen moeten worden (Snedaker, 2014).

In overleg met de opdrachtgever zijn de volgende verantwoordelijkheden toegevoegd: wanneer het DRP in het geval van een calamiteit is geactiveerd -- door het ‘damage assessment team’ -- dient het ‘IT recovery team’ de herstelprocedures uit te voeren (d.w.z. procedures die betrekking hebben op het herstellen van IT apparatuur, bijv. servers en switches). M.b.t. het herstel van de IT systemen (a.d.h.v. de omschreven herstelprocedures) dient in alle gevallen een switch, een VMware server en een SAN opslag systeem beschikbaar te zijn, zodat de systemen elkaar kunnen benaderen om bijv. de back-up terug te kunnen plaatsen (C. Bruntink, persoonlijke mededeling, 1 december 2015).

De status van de herstelprocedures dient te worden gerapporteerd aan het ‘management team’. Wanneer de herstelprocedures zijn voltooid en IT systemen zijn hersteld (en dus de bedrijfsvoering), dient dit gemeld te worden aan het ‘management team’ en het ‘functional area team’. De ondernomen stappen gedurende de herstelprocedures dienen te worden gedocumenteerd en gemeld aan het ‘management team’.

6.2.4 Functional area team

In overleg met de opdrachtgever is het ‘functional area team’ samengesteld. Het ‘functional area team’ bestaat uit de managers van de afdelingen verkoop, inkoop, magazijn en administratie waarbinnen zich de kritische bedrijfsprocessen bevinden van Tsubakimoto. Het ‘functional area team’ is in het geval van calamiteiten verantwoordelijk haar personeel zoveel mogelijk in staat te stellen de werkzaamheden te hervatten. Daarnaast is het ‘functional area team’ ook verantwoordelijk voor het onderhouden van de communicatie met klanten en leveranciers.

7. Conclusies en aanbevelingen

In dit hoofdstuk worden de belangrijkste conclusies omschreven welke gedurende de uitvoering van het afstudeerproject naar voren zijn gekomen. Daarnaast is in de vorm van aanbevelingen een advies uitgebracht m.b.t. het nemen van preventieve maatregelen tegen calamiteiten op lange termijn, en hoe het DRP moet worden opgevolgd.

7.1 Conclusie

In het DRP dient onder meer omschreven te worden onder welke omstandigheden het plan geraadpleegd dient te worden, hoe het stafpersoneel dient te handelen in geval van calamiteiten, welke maatregelen genomen moeten worden om het risico op calamiteiten te verminderen (en mogelijk te voorkomen), en hoe de herstelprocedures m.b.t. de IT apparatuur verlopen.

Voordat is gestart aan de realisatie van het DRP, zijn de kritische bedrijfsprocessen binnen Tsubakimoto omschreven. De kritische bedrijfsprocessen hebben betrekking op de facturatie en levering van goederen aan de klant. Wanneer de kritische bedrijfsprocessen in het geval van een calamiteit niet uitgevoerd kunnen worden, betekent dit dat Tsubakimoto niet in staat is goederen te factureren en te leveren, met als mogelijk gevolg klanten en inkomsten te verliezen.

Voorafgaand aan de uitvoering van de risicoanalyse, zijn vervolgens de bedrijfskritische IT systemen en componenten in kaart gebracht die de kritische bedrijfsprocessen ondersteunen. Deze apparatuur omvat zowel fysieke als virtuele servers, switches, de router en de firewall. Middels het uitvoeren van een risicoanalyse zijn vervolgens de calamiteiten geïnventariseerd welke een fysieke impact hebben op de IT systemen, componenten en data. Om middels meetbare resultaten aan te tonen wat de kans (op jaarbasis) en de impact (uitgedrukt in hardware kosten en kosten aan verloren manuren) is van de risico's op calamiteiten, is gebruik gemaakt van de kwantitatieve methode. Nadat de risicoanalyse is afgerond, zijn vervolgens correctieve en preventieve maatregelen omschreven die het risico op calamiteiten minimaliseren en waar mogelijk kunnen voorkomen.

Met behulp van deze conclusies, kan vervolgens een antwoord worden gegeven op de onderzoeksvraag. De onderzoeksvraag is tweedelig: *Welke maatregelen zijn noodzakelijk om enerzijds het risico op calamiteiten te minimaliseren [1] en anderzijds adequaat in te grijpen bij calamiteiten [2]?*

[1] Er zijn verschillende maatregelen die genomen kunnen worden om de risico's op calamiteiten te minimaliseren en mogelijk te voorkomen:

- Een virusaanval of onopzettelijk handelen door personeel, kan dataverlies veroorzaken. Om het risico op een virusaanval te minimaliseren, dient er meer bewustzijn onder het personeel gecreëerd te worden. Om dataverlies te voorkomen, dienen regelmatiger back-ups uitgevoerd te worden.
- Uitval van IT apparatuur kan worden veroorzaakt door diefstal, brand of hardware falen. Door bij voorbaat vervangende IT apparatuur aan te schaffen, kan systeemuitval worden voorkomen. Daarnaast kan het risico op diefstal van IT apparatuur worden verminderd, door de stellingen in de server ruimtes te voorzien van een slot.
- Het risico op een stroomstoring of hardware falen kan worden geminimaliseerd door de IT apparatuur regelmatiger te onderhouden, waardoor potentiële defecten tijdig hersteld kunnen worden. Daarnaast dient verouderde hardware in gebruik vervangen te worden, wat het risico op hardware falen verminderd.

[2] De verantwoordelijken binnen Tsubakimoto dienen als volgt in te grijpen in het geval van calamiteiten; wanneer een calamiteit zich voordoet, dient eerst de ernst van de situatie te worden ingeschat. Wanneer het DRP in werking is getreden, moet de impact op de IT apparatuur (en eventueel data) worden vastgesteld. Hierbij dienen klanten en leveranciers op de hoogte te worden gebracht van de situatie. Afhankelijk van de situatie dienen maatregelen genomen te worden om verdere schade te voorkomen. Om de IT apparatuur en data te herstellen, moeten de herstelprocedures zoals is omschreven in het DRP worden uitgevoerd. Wanneer de situatie is hersteld, dienen de ondernomen stappen voor herstel te worden gedocumenteerd in de vorm van een logboek.

7.2 Aanbevelingen

Aanbevelingen m.b.t. het nemen van preventieve maatregelen op lange termijn:

- Voer een *penetratietest* uit om eventuele kwetsbaarheden m.b.t. de beveiliging van IT systemen te detecteren. Hierdoor wordt voorkomen dat kwaadwillende personen (bijv. hackers) deze kwetsbaarheden misbruiken om de beveiliging van IT systemen te doorbreken, omzeilen of in te breken met als doel zoveel mogelijk schade te veroorzaken (bijv. het stelen van bedrijfsgegevens).

- Het implementeren van een 'failover' internetverbinding geeft een betere garantie voor de continuïteit van de bedrijfsvoering. In het geval de netwerk connectiviteit uitvalt, neemt de secundaire verbinding de functionaliteit over waardoor verlies van netwerk connectiviteit wordt voorkomen.

- Het is aan te raden een alternatieve werklocatie in te richten, om te voorkomen dat de bedrijfsvoering voor een lange periode niet functioneert. Door te beschikken over een alternatieve werklocatie kunnen de IT systemen en componenten (en dus de bedrijfsvoering) zo snel mogelijk worden hersteld in het geval van een desastreuze calamiteit (een brand ontstaan in de server ruimte kan tenslotte uitbreiden tot in de gehele faciliteit). Hierin zijn drie varianten te onderscheiden die toegepast kunnen worden:
    - '*Hot Site*' (door de IT omgeving te repliceren naar het externe datacenter, blijven de servers en de back-up omgeving functioneren);
    - '*Warm Site*' (middels een pre-installatie van de hardware- en brandbreedte configuratie, kan de software en data worden ingeladen in de IT systemen);
    - '*Cold Site*' (de hardware verplaatsen naar een alternatieve werkruimte die op voorhand beschikt over stroomvoorzieningen en netwerk connectiviteit).

- De router en de firewall die momenteel geïmplementeerd zijn binnen de netwerkinfrastructuur zijn verouderd, wat het risico op systeem falen en verlies van netwerk connectiviteit vergroot. Het is aan te raden een vervangende router en firewall aan te schaffen. Door op voorhand te beschikken over een (tevens vooraf geconfigureerde) router en firewall, kan systeem falen worden voorkomen.

- De '*core switch*' van het netwerk is niet redundant uitgevoerd. Indien deze switch uitvalt, is de communicatie tussen de servers en de netwerk connectiviteit verstoord. Het is daarom aan te bevelen een tweede 'core switch' in het netwerk te implementeren. In het geval een switch uitvalt, neemt de secundaire switch de functionaliteit over waardoor uitval van (netwerk) connectiviteit wordt voorkomen.

Aanbevelingen m.b.t. het Disaster Recovery plan:

- Nu er een DRP is gerealiseerd, dient deze vervolgens getest te worden. Hiervoor kan een zogenaamde '*roll-back*' test worden uitgevoerd. Dit houdt in dat een calamiteit wordt gesimuleerd (bijv. diefstal van IT apparatuur), waarin onder meer wordt getest hoe lang het duurt om te herstellen van calamiteiten, en of de omschreven herstelprocedures in het DRP effectief zijn in de praktijk. Daarnaast kan op deze wijze ook het stafpersoneel binnen Tsubakimoto worden getraind zodat zij zich bewust worden van hun verantwoordelijkheden.

- Het is aan te raden het DRP zeer regelmatig te herzien en direct bij te werken wanneer er wijzigingen plaatsvinden in bijvoorbeeld de IT omgeving (bijv. implementatie van nieuwe apparatuur). Hierbij dient met name ook de risicoanalyse te worden herzien en zoveel mogelijk uitgebreid te worden. Dit draagt uiteindelijk bij aan een effectiever DRP.

- Onderzoek hoe er alsnog een passende oplossing gerealiseerd kan worden wat betreft het herstellen van de configuratie van de SAN opslag omgeving. Helaas was het gedurende het onderzoek niet gelukt een oplossing hiervoor te vinden.

8. Evaluatie procesgang

In dit hoofdstuk is de evaluatie van de procesgang van het afstudeerproject omschreven. De zelfreflectie is te vinden in de appendix.

Plan van Aanpak
Het Plan van Aanpak was een belangrijke leidraad gedurende het afstudeeronderzoek. Ik zag dit als een essentieel document, omdat in hierin onder meer de concrete afbakening van het afstudeerproject is omschreven. Ik vond het voornamelijk in de beginfase van het afstudeerproject lastig om een goede en concrete afbakening te definiëren in het Plan van Aanpak, omdat het afstudeeronderzoek een erg grootschalig onderwerp omvat. Dankzij de feedback van mijn docentbegeleider heb ik hiervan uiteindelijk wel een concreet beeld kunnen vormen, en was ik tevreden met het resultaat.

Communicatie
De communicatie gedurende het afstudeerproject is prima verlopen, ik was gedurende de gehele afstudeerperiode werkzaam op de ICT afdeling -- onder meer samen met mijn bedrijfsbegeleider -- wat de communicatie onderling zeker ten goede kwam. Ik kon ook altijd bij hem terecht voor vragen of feedback. Wekelijks vonden er ook terugkoppelingen plaats met mijn bedrijfsbegeleider, om de voortgang te bespreken en om te toetsen of de op te leveren producten nog voldeden aan de eisen en verwachtingen volgens de kwaliteitscriteria in het Plan van Aanpak.

Om de twee weken heb ik mijn docentbegeleider ook op de hoogte gehouden van de voortgang. Wanneer ik vragen had of ergens mee vast kwam te zitten, was mijn docentbegeleider ook goed bereikbaar wat ik als zeer prettig heb ervaren. Daarnaast vond ik het ook erg prettig dat mijn docentbegeleider altijd ruim op tijd was met het geven van feedback op de door mij aangeleverde documentatie.

Planning
Er zijn geen grote verschillen opgetreden tussen de door mij beoogde en uiteindelijk gerealiseerde procesgang. Ik hield mijn planning zeer nauw in de gaten, en toetste zeer regelmatig met mijn bedrijfsbegeleider of hij mijn planning bijv. relevant vond en of ik de (deel)producten op tijd af zou krijgen. Achteraf ben ik echter wel blij dat ik een week uitloop heb ingepland, want dat was wel nodig geweest. Sommige deelproducten waren tegen de verwachting in toch wat uitgelopen wat betreft de oplevering, omdat ik gedurende de uitvoering tot nieuwe inzichten kwam, of omdat het onderzoeken van sommige aspecten toch iets langer duurde dan vooraf verwacht. Dit had echter geen effect op de eindresultaten, behalve dat sommige onderdelen iets later werden opgeleverd dan verwacht.

Inhoud onderzoek
Het onderzoek is gestart met het verrichten van een vooronderzoek, waarin ik voornamelijk heb onderzocht hoe een Disaster Recovery plan gerealiseerd kon worden, en hoe de risicoanalyse kon worden uitgevoerd. Dit was een zeer belangrijke eerste stap, omdat dit bepalend was voor de invulling van het eindproduct (het DRP). Uiteindelijk heb ik erg veel bruikbare informatie kunnen vinden in dit stadium, en was dit een goede basis voor de start van mijn afstudeeropdracht.

Na het afronden van het vooronderzoek ben ik gestart met het uitwerken van het verloop van de kritische bedrijfsprocessen. Ik had hier achteraf gezien wel iets eerder mee willen beginnen, maar doordat ik meer tijd had gestoken in het vooronderzoek dan verwacht, was ik iets later begonnen met het beantwoorden van dit onderdeel.

Na het afronden van de omschrijving van de kritische bedrijfsprocessen ben ik direct begonnen aan het in kaart brengen van de IT systemen en componenten. Het was een leerzame en tijdrovend onderdeel, omdat ik van een groot aantal systemen veel verschillende specificaties heb gedocumenteerd. Het was wel erg leerzaam en leuk om te doen. Dit onderdeel was ook iets eerder dan verwacht afgerond, waardoor ik eerder kon starten met de risicoanalyse.

De risicoanalyse was wel een van de lastige aspecten, omdat ik en mijn bedrijfsbegeleider van tevoren goed hadden nagedacht over de methode die zou worden toegepast. Hierbij vond ik het belangrijk dat de resultaten (concreet) bruikbaar waren voor de organisatie, en dat ik tegelijkertijd de resultaten ook kon onderbouwen. Omdat het wat tijd heeft gekost om de juiste aanpak en afbakening van de risicoanalyse te bepalen, was met name dit onderdeel van de opdracht wat uitgelopen (en duurde de uitwerking langer dan verwacht). Het resultaat is echter wel precies wat mijn bedrijfsbegeleider en ik voor ogen hadden, en ben ik blij met het resultaat.

Het uiteindelijk realiseren van het Disaster Recovery plan was een leuke en leerzame uitdaging. Ik had er vooraf op gerekend dat dit het meeste tijd zou kosten, en hier dan ook veel tijd voor ingepland. Gedurende het realiseren van het plan ben ik gelukkig niet tegen problemen aangelopen (dat ik bijv. niet wist hoe het verder zou moeten), omdat ik een redelijk uitgebreid vooronderzoek had verricht. Daarnaast had mijn bedrijfsbegeleider ook een boek speciaal hiervoor aangeschaft wat ik zeer heb gewaardeerd, wat mij goed heeft ondersteund in het realiseren van dit plan (samen met de inzet van mijn bedrijfsbegeleider). Het plan was echter wel iets later afgerond dan gepland, met name omdat het laatste stadium (formuleren van herstelprocedures) veel tijd heeft gekost en er op het laatste moment nog wat wijzigingen werden doorgevoerd, maar ik ben erg trots op het eindresultaat.

Gedurende het afstudeerproject ben ik tijdig begonnen met het opstellen van het adviesrapport en de scriptie. Ik heb hier ook erg veel tijd voor genomen (en er voornamelijk in mijn vrije tijd aan gewerkt). Dit heeft mij wel erg geholpen, want doordat ik er veel tijd in heb gestoken en er vroeg aan ben begonnen, ben ik niet in tijd nood gekomen.

Bronvermelding

Axis Insurance. (z.d.). *Water damage - loss control*. Gedownload op 25 november 2015, van http://www.axisinsurance.ca/images/uploads/Water_Damage_Loss_Control.pdf

Brakel Atmos. (z.d.). Snelle detectie - rookdetectie en branddetectie - redt levens! Geraadpleegd op 25 november 2015, van https://www.brakelatmos.com/nl/nl/4/snelle-detectie-rookdetectie-en-branddetectie-redt-levens

Castagna, R. (2015). Need a Disaster Recovery plan? You're not alone. Geraadpleegd op: http://searchdisasterrecovery.techtarget.com/feature/Need-a-business-disaster-recovery-plan-Youre-not-alone

CBS. (2015). *Steeds meer ondernemers in Nederland* [Persbericht]. Geraadpleegd op: http://www.cbs.nl/nl-NL/menu/themas/bedrijven/publicaties/artikelen/archief/2015/steeds-meer-ondernemers-in-nederland.htm

ElektricienNu. (z.d.). Kortsluiting. Geraadpleegd op 25 november 2015, van http://www.elektricien-nu.nl/kortsluiting/

Fire prevention. (z.d.). Geraadpleegd op 25 november 2015, van http://www.dayjob.com/content/fire-prevention-191.htm

Harbaugh, L, G. (2009). Reduce chances of hardware failure with preventive server maintenance. Geraadpleegd op 28 november 2015, van http://searchdatacenter.techtarget.com/tip/Reduce-chances-of-hardware-failure-with-preventive-server-maintenance

Hiscox. (z.d.). Waterschade. Geraadpleegd op 25 november 2015, van http://www.hiscox.nl/particuliere-verzekeringen/tips-en-services/waterschade/

Interpolis. (2012). Zakelijke inbraken in kaart. Geraadpleegd op: https://www.interpolis.nl/zakelijk/inzicht/kenniscentrum/thema/inbraak-en-diefstal/zakelijke-inbraken-in-kaart/paginas/default.aspx

Kennisconsult. (2011). Watervalmethode. Geraadpleegd op: http://www.kennisconsult.nl/begrippen/5028/

Mitre. (z.d.). Risk Process Guidelines. Gedownload op 22 november 2015, van http://www2.mitre.org/work/sepo/toolkits/risk/compliance/files/RiskProcessGuidelines.doc

Netbeheer Nederland. (2014). *Betrouwbaarheid van elektriciteitsnetten in Nederland. Resultaten 2014*. Gedownload op 16-11-2015, van http://www.netbeheernederland.nl/publicaties/onderzoek/

NIST. (2012). *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30 Rev. 1). Gedownload op 21 september 2015, van http://csrc.nist.gov./publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Ombudsman van de Verzekeringen. (2014). *Cijfers en analyse 2014*. Gedownload op 16-11-2015, van http://www.ombudsman.as/nl/documents/Rapport_Ombudsman_2014.pdf

Snedaker, S., Rima, C. (2014). *Business Continuity and Disaster Recovery Planning for IT Professionals* (Second ed.). Waltham, MA: Syngress.

Swanson, M., Bowen, P., Wohl-Phillips, A., Gallup, D. & Lynes, D. (2010). *Contingency Planning Guide for Federal Information Systems* (NIST Special Publication 800-34 Rev. 1). Gedownload op 21 September 2015, van http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Tsubakimoto Chain Co. (2008). *Tsubaki Corporate Ethics Handbook*.

Tsubakimoto Europe B.V. (2015). Geraadpleegd op: http://tsubaki.eu/

Tsubakimoto Europe B.V. (2014). RE-10-4510-W-001-J - Back-up procedure.igx. Geraadpleegd op: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2014). RE-1-0060-W-001 - Control debtors.igx. Geraadpleegd op: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-3-1040-W-001 - Creating article record.igx. Geraadpleegd op: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-7-3003-W-001-K Manual Creditor payment.igx. Geraadpleegd op: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2013). RE-1-0050-W-001-K Margin control and invoicing.igx. Geraadpleegd op: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-5-2000-W-001-K Order collection, packaging and shipment.igx. Geraadpleegd op: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-3-1000-W-001-J Purchase order.igx. Geraadpleegd op: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2013). RE-5-2020-W-001-K Receipt goods and warehousing.igx. Geraadpleegd op: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2014). RE-10-4515-W-001-J - Restore procedure.igx. Geraadpleegd op: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-1-0020-W-001-J Sales order.igx. Geraadpleegd op: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-1-0010-W-001-J Sales quotation.igx. Geraadpleegd op: http://datasrv03/Tsubaki%20intranet/index.html

VEBON. (2014). Bedrijfsbranden. Geraadpleegd op: http://vebon.org/kennisbank/feiten---cijfers/brand/bedrijfsbranden?id=1821

Vereniging beheer Dordtse Kil III. (2009). Bedrijventerrein "Kil III". Geraadpleegd op: http://www.vereniging-dordtsekil3.nl/bedrijven-0413_A.html

Begrippenlijst

Bottleneck	Een knelpunt (of kwetsbaarheid) binnen een proces, project of systeem (bron: http://www.betekenis-definitie.nl/bottleneck)	*p. 24*
Business Continuity plan (BCP)	Een Business Continuity plan richt zich op de instructies en/ of procedures die beschrijven hoe de missie en de bedrijfsprocessen van een organisatie (als geheel) tijdens en na een verstoring worden ondersteund (bron: NIST, 2010)	*p. 10*
Cold Site	Een alternatieve werkruimte die op voorhand beschikt over stroomvoorzieningen en netwerk connectiviteit (bron: http:// www.corexchange.com/blog/disaster-recovery-hot-warm-cold-sites-key-differences)	*p. 38*
Core switch	Een switch die zich over het algemeen in de kern van een netwerk bevindt (bron: https://www.techopedia.com/definition/28787/core-switch-networking)	*p. 38*
Disaster Recovery plan (DRP)	Een Disaster Recovery plan is gericht op het herstel van de functionaliteit van IT computer systemen en componenten na een calamiteit. Het DRP richt zich op calamiteiten op het gebied van IT (bron: NIST, 2010)	*p. 9*
Failover	Een back-up methode waarmee de functionaliteit van een IT systeem wordt overgenomen door een secundair systeem wanneer het primaire systeem niet beschikbaar is (bron: http://searchstorage. techtarget.com/definition/failover)	*p. 22*
Full back-up	Een totale back-up van alle bestanden (dus niet alleen van bestanden die zijn gewijzigd sinds de laatste back-up) (bron: http://www.computerwoorden.nl/direct--9729--Full%20backup.htm)	*p. 20*
Hacking	Iemand die probeert toegang te krijgen tot een IT systeem of gegevens van iemand anders, via het gebruik van computers en netwerken (bron: http://www.vraaghetdepolitie.nl/sf.mcgi?238)	*p. 25*
Hot Site	Een extern datacenter waarnaar de IT omgeving gerepliceerd kan worden zodat de servers en de back-up omgeving blijven functioneren (bron: http://www.corexchange.com/blog/disaster-recovery-hot-warm-cold-sites-key-differences)	*p. 38*
Incrementele back-up	Een back-up waarbij, sinds de laatste full back-up, alleen de nieuwe en gewijzigde bestanden worden gekopieerd (bron: http://www.computerwoorden.nl/direct--11111--Incremental%20backup.htm)	*p. 20*
Load balance	Load balancing verdeelt de hoeveelheid werk die een computer moet verwerken, tussen twee of meer computers waardoor meer werk kan worden voltooid in dezelfde hoeveelheid tijd (bron: http://searchnetworking.techtarget.com/definition/load-balancing)	*p. 22*
OEM	(Original Equipment Manufacturer. Ook wel: “Onder Eigen Merk”) Producten die worden geleverd aan andere fabrikanten welke worden geïntegreerd in hun eigen producten (bron: http://www.webwoordenboek.be/verklaringen/oem/)	*p. 9*
Off-site	(Op het gebied van back-ups) Een off-site back-up omvat een externe organisatie die de back-ups beheerd (bron: https://www.techopedia.com/definition/30124/offsite-backup)	*p. 21*
Penetratietest	Een controle van computer systemen, waarbij wordt onderzocht of kwetsbaarheden kunnen worden misbruikt om onder meer de beveiliging te omzeilen (bron: http://www.auditconnect.nl/nl/it-audits/penetratietest/)	*p. 38*
Phishing	Phishing is een vorm van internetfraude waarbij derden via bijv. valse e-mail berichten vertrouwelijke informatie achterhalen (bron: https://www.mediawijsheid.nl/phishing/)	*p. 25*
Replicatie	Het synchroniseren van data, waardoor back-ups efficiënt kunnen worden beheerd (bron: http://www-01.ibm.com/software/data/replication/)	*p. 20*
Roll-back test	Het simuleren van een calamiteit om te testen hoe lang het duurt om te herstellen van calamiteiten (bron: http://www.aterion.nl/ict-oplossingen/disaster-recovery.php)	*p. 39*

Thin client	Een thin client is een desktop terminal die geen harde schijf bevat. Alle functies die zijn te vinden op een desktop pc (zoals toepassingen en data) kunnen door een thin client worden benaderd, doordat deze functies zijn opgeslagen in een datacenter (bron: http://www.devonit.com/thin-client-education)	*p. 21*
Tools	Een tool is een hulpprogramma die bepaalde handelingen gemakkelijker maken voor gebruikers (bron: http://www.computerwoorden.nl/direct--15981--Tool.htm)	*p. 33*
Warm Site	Het inladen van software en data in de IT systemen, door te beschikken over een pre-installatie van de hardware- en brandbreedte configuratie (bron: http://www.corexchange.com/blog/ disaster-recovery-hot-warm-cold-sites-key-differences)	*p. 38*

Overzicht van tabellen en figuren

Tabellen

Figuren

Bijlage A - Plan van Aanpak

1. Inleiding

Dit document omschrijft het Plan van Aanpak (PvA) voor het afstudeerproject "Disaster Recovery planning", welke zal worden uitgevoerd bij Tsubakimoto Europe B.V. te Dordrecht. De organisatie beschikt momenteel niet over een Disaster Recovery plan, noch de capaciteit om deze te ontwikkelen.

Omdat het ontbreken van een Disaster Recovery plan (DRP) desastreuze gevolgen kan hebben voor het voortbestaan van de organisatie (bijv. imagoschade doordat de primaire bedrijfsprocessen na uitval van IT systemen door een calamiteit niet meer kunnen functioneren), is dit project tot stand gekomen. Het is van belang dat de verantwoordelijken binnen de organisatie weten hoe gehandeld dient te worden in het geval van een calamiteit en welke maatregelen genomen kunnen worden om de schade te beperken (en zo mogelijk te voorkomen). Deze aspecten zullen uiteindelijk worden opgenomen in een Disaster Recovery plan welke aan het einde van het afstudeerproject zal worden opgeleverd aan de organisatie.

Leeswijzer

In hoofdstuk 2 komt de context van de opdracht aan de orde waarin de organisatie zal worden omschreven met daarbij de aanleiding, kwestie en doelstellingen van de opdracht.

In hoofdstuk 3 wordt de opdracht omschreven met daarin de onderzoeksvragen, op te leveren producten, onderzoeksresultaten, onderzoeksmethoden en het theoretisch kader.

In hoofdstuk 4 zijn de projectactiviteiten uiteen gezet met daarin opgenomen de fasering, projectrisico's en communicatie.

In hoofdstuk 5 zijn de randvoorwaarden opgesteld en wordt de afbakening van het project beknopt omschreven.

In hoofdstuk 6 is de projectplanning schematisch weergegeven.

2. Context

In dit hoofdstuk wordt de context van de opdracht omschreven. Hierin komen onderwerpen aan de orde m.b.t. de omschrijving van de organisatie en de aanleiding tot de opdracht.

2.1 Organisatie omschrijving

2.1.1 Over Tsubakimoto Europe B.V.

Tsubakimoto Europe B.V. is opgericht in 1972 en gevestigd te Dordrecht. Tsubakimoto Europe B.V. is onderdeel van de Tsubakimoto Chain Company en opereert naast Europa in de volgende werelddelen: Rusland, Afrika en het Midden-Oosten (met uitzondering van de Europese landen die al worden bediend door een andere maatschappij van Tsubakimoto). Tsubakimoto Europe B.V. wordt ondersteunt door lokale vestigingen in het Verenigd Koninkrijk en Duitsland. De vestiging in Dordrecht is tevens het hoofdkantoor van de Europese tak van de organisatie (Tsubakimoto Europe B.V., 2015).

Tsubakimoto Europe B.V. verzorgt de distributie van industriële aandrijfkettingen en aanverwante producten aan distributeurs en OEM's. Tsubakimoto Europe B.V. beschikt ook over een moderne werkplaats waar assemblage werkzaamheden worden verricht op de producten voor kant-en-klaar gebruik. Binnen de vestiging in Dordrecht zijn circa 70 medewerkers werkzaam.

Tsubakimoto beschikt binnen Europa over de volgende kantoren:

- Tsubakimoto Europe B.V. (TEU), gevestigd te Dordrecht.
  - Gericht op de klanten binnen de Europese markt.
- Tsubakimoto U.K. (TUK), gevestigd te Nottingham.
  - Gericht op de klanten in het Verenigd Koninkrijk, Ierland en IJsland.
- Tsubaki Deutschland GmbH (TDEG), gevestigd te Gilching (Beieren).
  - Gericht op de klanten in Duitsland.

2.1.2 De ICT omgeving

Binnen de ICT afdeling van de organisatie zijn de IT manager en de IT system engineer actief. De IT manager is verantwoordelijk voor de optimalisatie van de bedrijfsprocessen, beschikbare IT capaciteit en uitvoeren van ICT projecten. Daarnaast ondersteunt de IT manager ook de eindgebruikers binnen de organisatie. De IT system engineer ondersteunt de IT manager in de werkzaamheden op het gebied van de optimalisatie van de bedrijfsprocessen en IT capaciteit binnen de organisatie. Het installeren, inrichten en beheren van de hard- en software alsmede de ondersteuning voor de eindgebruikers hoort ook bij de verantwoordelijkheden van de IT system engineer.

Het project zal worden uitgevoerd binnen de ICT afdeling. Zowel de IT manager (tevens de bedrijfsbegeleider) als de systeem- en netwerkbeheerder (IT system engineer) zijn actief binnen deze afdeling en zijn beschikbaar om de student gedurende de uitvoering van het project te ondersteunen. Indien er meer afdelingen zijn binnen de organisatie die deel uitmaken van het project, of wanneer medewerkers van andere afdelingen een bijdrage kunnen leveren aan de opdracht, zal er ook de ruimte zijn deze afdelingen bij het project te betrekken. In Bijlage 1: Organigram Tsubakimoto Europe B.V. is de organisatiestructuur weergegeven.

Wat betreft de ICT omgeving en netwerk-infrastructuur zijn onderstaande ICT systemen/ componenten binnen Tsubakimoto Europe B.V. gerealiseerd:

- Het netwerk bestaat onder meer uit 7 fysieke servers, waarvan twee servers zijn gebaseerd op VMWare ESX. De overige servers zijn gebaseerd op Windows Server 2008/ 2012. Daarnaast zijn er nog 15 virtuele servers, 49 PC's, 17 Thin Clients en 49 laptops
- Er zijn twee computerruimtes, waarvan de tweede ruimte dient als failover.

- Het netwerk beschikt over Cat5e bekabeling, een Areohives WLAN en HP Procurve switches. Wat betreft de internet connectiviteit is er een 20 MB glasvezel verbinding en een 100 MB glasvezel verbinding aangelegd.
- De organisatie beschikt ook over een (centraal gelokaliseerd en beheerd) ERP-systeem waaraan, middels een Citrix omgeving, de vestigingen in het Verenigd Koninkrijk en Duitsland zijn gekoppeld. Daarnaast heeft de organisatie de ICT omgeving van de vestiging in Duitsland lokaal in beheer. De vestiging in het Verenigd Koninkrijk beschikt over een eigen ICT omgeving (behalve het ERP-systeem). Wanneer er echter problemen ontstaan m.b.t. het ERP-systeem (en de Citrix omgeving), zullen de vestigingen in zowel het Verenigd Koninkrijk als Duitsland hiervan ook hinder ondervinden.

2.2 Aanleiding opdracht

Binnen de ICT afdeling van Tsubakimoto Europe B.V. zijn twee medewerkers actief die verantwoordelijk zijn voor de ICT omgeving. Tot op heden zijn er nog geen grote ICT calamiteiten voorgevallen binnen de organisatie (bijv. brand in de server ruimte), maar de directie van de organisatie en accountants vinden het wenselijk is dat er op korte termijn een Disaster Recovery plan wordt gerealiseerd. De reden dat dit noodzakelijk wordt geacht vanuit de directie en accountants, is omdat de organisatie de intentie heeft om te werken aan een Business Continuity plan (BCP), waarvoor een Disaster Recovery plan benodigd is.

Om het verschil aan te duiden tussen een Disaster Recovery plan (DRP) en een Business Continuity plan (BCP) zijn deze begrippen onderstaand gedefinieerd als volgt:

Een Disaster Recovery plan is enkel gericht op het herstel van de functionaliteit van computer systemen/ componenten en andere IT gerelateerde apparatuur na een calamiteit. Het DRP richt zich uitsluitend op calamiteiten op het gebied van IT (NIST, 2010).

Een Business Continuity plan richt zich op de instructies en/ of procedures die beschrijven hoe de missie en de bedrijfsprocessen van een organisatie (als geheel) tijdens en na een verstoring worden ondersteund (NIST, 2010).

2.2.1 De kwestie

Momenteel beschikt de organisatie niet over de capaciteit om zelf een DRP te ontwikkelen, waardoor externe hulp benodigd is om het project uit te voeren. Het is voor de organisatie nog onduidelijk welke mogelijke calamiteiten zich kunnen voordoen binnen de ICT omgeving en hoe de verantwoordelijken hierbij moeten ingrijpen, omdat de organisatie niet beschikt over een DRP. Het ontbreken van een DRP kan ernstige gevolgen hebben voor de organisatie wanneer er calamiteiten optreden binnen de ICT omgeving (bijv. imagoschade doordat de primaire bedrijfsprocessen niet functioneren). Het is hierbij belangrijk dat de verantwoordelijken binnen de organisatie weten hoe zij dienen te handelen in het geval van een calamiteit en welke maatregelen genomen dienen te worden om deze calamiteiten effectief aan te pakken (en waar mogelijk te voorkomen).

2.2.2 Doelstellingen organisatie

M.b.t. de productie en levering aan de klant, zijn bedrijfsprocessen gemoeid die niet kunnen functioneren zonder ICT systemen en/of componenten. Wanneer calamiteiten zich voordoen binnen de ICT omgeving, kan dat dus ook negatieve gevolgen hebben voor zowel de productie (en levering) van goederen als voor de klanten. Hierdoor kan de missie van de organisatie niet worden nagestreefd; A-merk producten van hoge kwaliteit leveren aan de klant.

De organisatie wil een Disaster Recovery plan implementeren om minder kwetsbaar te worden voor risico's binnen de ICT omgeving. Door de risico's in kaart te brengen kunnen calamiteiten tijdig worden gesignaleerd om de schade te beperken en (waar mogelijk) te voorkomen, zodat de bedrijfsprocessen (en uiteindelijk dus de klanten) hiervan zo min mogelijk hinder ondervinden. Hierbij gaat het om de calamiteiten welke hun oorzaak vinden in de ICT omgeving (zoals hardware falen, diefstal van IT gegevens) maar ook om de calamiteiten welke gevolgen zullen hebben voor de ICT omgeving (zoals een brand in de server ruimte). Daarnaast wil de organisatie dat wordt omschreven hoe de verantwoordelijken binnen de organisatie dienen te handelen in het geval van ICT

gerelateerde calamiteiten, zodat de bedrijfsvoering zo snel mogelijk hersteld kan worden naar de oorspronkelijke situatie.

Opdracht
De volgende onderdelen dienen gerealiseerd te zijn om de opdracht geslaagd te kunnen noemen:

- Een inventarisatie van de IT infrastructuur met de daarbij behorende bedrijfskritische systemen/ componenten die de primaire bedrijfsprocessen ondersteunen;
- Risicoanalyse (aan welke mogelijke bedreigingen de ICT systemen/ componenten blootstaan);
- Een actueel en onderhoudbaar DRP welke als draaiboek fungeert in geval van ICT gerelateerde calamiteiten. Hierin moet duidelijk worden omschreven welke maatregelen genomen moeten worden door de verantwoordelijken binnen de organisatie (met daarbij de bijbehorende verantwoordelijkheden per persoon).
- Een adviesrapport waarin advies wordt gegeven hoe het DRP moet worden opgevolgd en onderhouden (zodat de organisatie in staat is het plan in te zetten in toekomstige situaties), en welke preventieve maatregelen genomen kunnen worden op lange termijn.

2.2.3 Type opdracht
Deze afstudeeropdracht omvat het verrichten van een descriptief onderzoek. Er is echter ook sprake van een ontwerponderzoek, omdat er uiteindelijk een nieuwe situatie wordt ontworpen (aan de hand van de omschreven maatregelen in het DRP en aanbevelingen in het adviesrapport). Middels het beantwoorden van de deelvragen, welke gericht zijn op het voorbereiden en realiseren van een DRP, wordt antwoord gegeven op de hoofdvraag.

3. Opdrachtomschrijving
De organisatie beschikt momenteel niet over een DRP welke kan worden toegepast wanneer ICT gerelateerde calamiteiten zich voordoen. Het is van groot belang dat de organisatie beschikt over een dergelijk plan, om adequaat te kunnen handelen in het geval van calamiteiten en daarmee desastreuze gevolgen (zoals imago schade doordat de primaire bedrijfsprocessen niet functioneren) voor de organisatie te voorkomen.

De opdracht kan als volgt worden geformuleerd:
Onderzoek welke maatregelen genomen dienen te worden om de risico's op ICT gerelateerde calamiteiten zoveel mogelijk in te perken en hoe de verantwoordelijken binnen de organisatie dienen in te grijpen in het geval wanneer calamiteiten optreden. Vervolgens kunnen op basis van de situatie, maatregelen worden genomen om te herstellen van calamiteiten en waar mogelijk preventieve maatregelen worden gedefinieerd om calamiteiten te voorkomen.

3.1 Onderzoeksvragen
3.1.1 Hoofdvraag
Voor dit afstudeeronderzoek is de volgende hoofdvraag geformuleerd:

"Welke maatregelen zijn noodzakelijk om enerzijds het risico op calamiteiten te minimaliseren en anderzijds adequaat in te grijpen bij calamiteiten?"

3.1.2 Deelvragen
Om antwoord te kunnen geven op deze hoofdvraag zijn de volgende deelvragen geformuleerd:

1. Hoe verlopen de primaire bedrijfsprocessen binnen de organisatie?
2. Welke bedrijfskritische systemen/ componenten zijn betrokken bij de primaire bedrijfsprocessen?
3. Welke ICT gerelateerde calamiteiten vormen een risico voor de bedrijfskritische systemen/ componenten?
4. Wat is de impact van de risico's op de bedrijfskritische systemen/ componenten en dus op de primaire bedrijfsprocessen?

5. Welke maatregelen dienen genomen te worden om het risico op calamiteiten te verminderen en waar mogelijk te voorkomen?
6. Hoe dienen de verantwoordelijken binnen de organisatie te handelen in het geval van een calamiteit?

3.1.3 Ethische afweging

Hoewel er geen directe relatie is tussen de problematiek en ethische aspecten (zoals duurzaamheid, sociaal-maatschappelijke of wetenschappelijke aspecten)dient de uitvoering van het project, de op te leveren producten voor de organisatie en het advies in lijn te zijn met de regelgeving van het bedrijf. Wat betreft de uitvoering van het project dienen de regels m.b.t. bescherming van bedrijfsmiddelen te worden gehandhaafd (waaronder producten, apparatuur, machines maar ook bedrijfsprocessen vallen). Door deze regels op te volgen moet verlies, misbruik of oneigenlijk gebruik van deze bedrijfsmiddelen worden voorkomen.

3.2 Producten

Gedurende het project zullen de volgende deelproducten worden opgeleverd:

- Vooronderzoek;
- Proces analyse & IT Componenten analyse;
- Risicoanalyse.

Aan het eind van het project worden onderstaande eindproducten opgeleverd:

- Een DRP;
- Een Adviesrapport;
- De Scriptie.

3.2.1 Relatie van deelvragen met producten

	Deelvraag	Product
1.	Hoe verlopen de primaire bedrijfsprocessen binnen de organisatie?	Proces analyse (Adviesrapport)
2.	Welke bedrijfskritische systemen/ componenten zijn betrokken bij de primaire bedrijfsprocessen?	IT Componenten analyse (Adviesrapport)
3.	Welke ICT gerelateerde calamiteiten vormen een risico voor de bedrijfskritische systemen/ componenten?	Risicoanalyse (Adviesrapport)
4.	Wat is de impact van de risico's op de bedrijfskritische systemen/ componenten en dus op de primaire bedrijfsprocessen?	Risicoanalyse (Adviesrapport)
5.	Welke maatregelen dienen genomen te worden om het risico op calamiteiten te verminderen en waar mogelijk te voorkomen?	Disaster Recovery plan (Adviesrapport)
6.	Hoe dienen de verantwoordelijken binnen de organisatie te handelen in het geval van een calamiteit?	Disaster Recovery plan (Adviesrapport)

3.2.2 MoSCoW analyse

Het vaststellen van prioriteiten aan de eisen van een project zijn belangrijk. Hierdoor wordt het namelijk mogelijk projecten hanteerbaar te houden. Vaak wordt hiervoor de MoSCoW analyse toegepast, waarbij deze eisen in de volgende categorieën worden ingedeeld:

Must Haves	De vereisten om tot een werkbaar product te komen
Should Haves	De vereisten die niet noodzakelijk zijn voor een functionerend eindproduct, maar die wel een hoge prioriteit hebben.
Could Haves	De vereisten die alleen worden meegenomen indien het haalbaar is binnen de tijd.
Would Haves	De vereisen die eventueel in de toekomst kunnen worden toegepast, maar die geen prioriteit hebben (MoSCoW-methode, z.d.).

De huidige onderdelen van de scope zijn van toepassing op dit project:

Must Haves:

- De resultaten van het afstudeeronderzoek (deelproducten, het DRP en het Adviesrapport) dienen te worden gerealiseerd binnen de afgesproken termijn.
- Wat betreft de Risicoanalyse en het DRP, worden de volgende calamiteiten onderzocht (welke relevant zijn voor de organisatie) en meegenomen in het project:
  - Calamiteiten welke hun oorzaak vinden in de ICT omgeving (bijv. hardware falen);
  - Calamiteiten die mogelijk gevolgen hebben voor de ICT omgeving (bijv. brand in server ruimte);
- Er dient een DRP te worden opgeleverd dat voldoet aan de gestelde eisen. Het DRP zal tevens onderdeel uitmaken van het Adviesrapport.
- M.b.t. de inhoud van het DRP (en de bijbehorende onderzoeken en (deel)producten) zullen alleen de ICT systemen/ componenten worden meegenomen die de primaire bedrijfsprocessen ondersteunen.

Should Haves:

- Het DRP dient in het Engels te zijn geschreven.
- Het DRP is bedoeld als leidraad voor de organisatie; en dient niet te uitvoerig (ingewikkeld) te zijn beschreven om complexiteit en onoverzichtelijkheid te vermijden.

Could Haves:

- Toevoegen van een mogelijk praktisch onderdeel aan de opdracht, bijvoorbeeld:
  - Het introduceren van failover in het bedrijfsnetwerk m.b.t. de internetverbindingen.

Would Haves:

- Het betrekken van software, de persoonlijke desktop computers en laptops van de medewerkers, alsmede de telefonie binnen de organisatie in de opdracht.
- Testen van het DRP.

3.3 Onderzoeksresultaten

3.3.1 Deelproducten met kwaliteitscriteria

- Vooronderzoek:
  - Analyse hoe een risicoanalyse kan worden uitgevoerd (bijv. met welke mogelijke technieken, richtlijnen) en welke aspecten deel uitmaken van een DRP (bijv. welke onderwerpen komen aan bod in een DRP, hoe is deze opgebouwd, welke aspecten in een DRP zijn relevant voor de organisatie?).
- Proces analyse & IT componenten analyse: analyseren wat de primaire bedrijfsprocessen zijn voor de organisatie, met de bijbehorende systemen/ componenten die deze processen ondersteunen.
  - Inventarisatie van de primaire bedrijfsprocessen;
  - Inventarisatie van de systemen/ componenten welke de bedrijfsprocessen ondersteunen (met daarbij bijv. specificaties, rollen, licenties etc.);
  - Inventarisatie van de leveranciers waarbij de apparatuur is aangeschaft.
- Risicoanalyse: omschrijft de mogelijke calamiteiten die zich kunnen voordoen binnen de ICT omgeving van de organisatie en welk effect deze calamiteiten hebben op de ICT systemen en primaire bedrijfsprocessen.
  - Mogelijke calamiteiten in kaart brengen welke een negatief effect hebben op de ICT systemen (en dus de primaire bedrijfsprocessen).
  - Inschatten wat de kans en impact van de calamiteiten zijn.
  - Inventarisatie van maatregelen om de impact van de calamiteiten te minimaliseren (en waar mogelijk direct te voorkomen).

3.3.2 Eindproducten met kwaliteitscriteria

- Disaster Recovery plan:
  - Omschrijft de stappen die nodig zijn om te herstellen na een calamiteit in de vorm van wat er moet gebeuren om een calamiteit aan te pakken en hoe dit moet verlopen. Hierin komt o.a. ook aan de orde hoe de verantwoordelijken binnen de organisatie dienen te handelen.
  - Het DRP zal zowel de correctieve, als de preventieve maatregelen omschrijven die voor de organisatie op korte termijn (direct) te realiseren zijn (een preventieve maatregel kan bijv. zijn dat de organisatie op voorhand beschikt over een extra server wanneer er een server uitvalt).
- Adviesrapport:
  - In het adviesrapport worden a.d.h.v. de resultaten van het onderzoek en de deelproducten, conclusies en aanbevelingen gegeven die betrekking hebben op het onderhoud en de implementatie van het Disaster Recovery plan.
  - In het adviesrapport worden -- in de vorm van aanbevelingen -- de preventieve maatregelen omschreven die de organisatie kan realiseren op lange termijn (bijv. een preventieve maatregel welke aanpassingen vraagt in de infrastructuur van de organisatie, wat geld gaat kosten en dus goedgekeurd moet worden door de directie en andere betrokken partijen).

3.3.3 Algemene kwaliteitscriteria

De volgende maatregelen worden toegepast om het project in goede banen te leiden en om de kwaliteit gedurende de uitvoer van het project te bewaken:

Omschrijving	Betrokken personen
Tijdens het onderzoek staan de onderzoeksvragen centraal. Hierbij dient voorkomen te worden dat er wordt afgeweken van het onderzoek (onderzoek alleen wat relevant is voor het beantwoorden van de hoofdvraag).	Student
Gedurende de uitvoer van het project zal er ook worden doorgewerkt aan de scriptie. Hiermee wordt voorkomen dat er bijv. te laat wordt gestart met de scriptie waardoor de uiteindelijke datum van oplevering niet kan worden behaald (tijd nood).	Student
Regelmatig contact onderhouden en duidelijke afspraken maken (met zowel de bedrijfsbegeleider als de docentbegeleider).	Student, Bedrijfsbegeleider, Docentbegeleider
Wekelijks communiceren over de voortgang van het project in de vorm van een (kort) gesprek met de bedrijfsbegeleider. Hierdoor kunnen eventuele problemen tijdig worden gesignaleerd, is er ruimte voor het geven van feedback en kan worden beoordeeld of het project nog voldoet aan de verwachtingen. Hieruit zal bijv. ook blijken of kan worden gestart met de volgende fase in het project.	Student Bedrijfsbegeleider
Regelmatig raadplegen van de planning om te toetsen of het project, met de bijbehorende werkzaamheden, nog verloopt volgens plan. Hierdoor kan tijdig worden vastgesteld of er bijv. onderdelen zijn die juist meer/ minder tijd in beslag nemen dan vooraf gedacht (en eventueel kan op basis hiervan in overleg met de bedrijfsbegeleider en docentbegeleider actie worden ondernomen).	Student, Bedrijfsbegeleider, (Docentbegeleider)
Waar nodig dienen de bedrijfsbegeleider, docentbegeleider, collega's en andere betrokkenen bereikbaar te zijn voor informatie, feedback en advies m.b.t. het uitvoeren van de opdracht.	Bedrijfsbegeleider, Docentbegeleider, Collega's, Leveranciers...
Alle producten worden eerst in conceptversie opgeleverd aan de bedrijfsbegeleider. Hierbij is het van belang dat de bedrijfsbegeleider beoordeelt (feedback) of deze producten voldoen aan de verwachtingen. **Het Adviesrapport en de Scriptie worden ook in conceptversie opgeleverd aan zowel de bedrijfsbegeleider als de docentbegeleider.*	Student, Bedrijfsbegeleider, Docentbegeleider

3.4 Onderzoeksmethoden

Voor dit project zal gebruik worden gemaakt van zowel kwalitatieve als de kwantitatieve onderzoeksmethoden. Bij kwalitatief onderzoek gaat het erom dat diepgaande informatie kan worden verzameld over een bepaald thema of vraagstuk. Kwalitatief onderzoek kan worden toegepast op onderzoeksvragen die antwoord moeten geven op vragen zoals 'waarom...?', 'welke...?', 'hoe...?', oftewel: die een probleem moeten oplossen. De meest voorkomende onderzoeksmethoden binnen kwalitatief onderzoek zijn onder meer: interviews, casestudies, observatie en literatuuronderzoek. Wat betreft het uitvoeren van de Risicoanalyse zal kwantitatief onderzoek worden toegepast, omdat de gegevens (zoals de risico's, impact en prioriteiten) worden uitgedrukt in cijfers. (Taalwinkel, z.d.).

Middels dit project dient er n.a.v. het uitvoeren van onderzoek op het gebied van o.a. het opstellen van een DRP en welke mogelijke bedreigingen binnen de IT kunnen voorkomen, uiteindelijk antwoord te worden gegeven op de hoofdvraag; **"Welke maatregelen zijn noodzakelijk om enerzijds het risico op calamiteiten te minimaliseren en anderzijds adequaat in te grijpen bij calamiteiten?"**

Betreffende dit project worden de volgende kwalitatieve onderzoeksmethoden worden toegepast:

- (Groeps)gesprekken/ Interviews:
  - Informatie verzamelen uit mededelingen van ondervraagde persoon(en) om een antwoord te kunnen geven op de geformuleerde vraagstukken over de probleemstelling.
- Observeren:
  - Op de werkvloer informatie verzamelen zodat kan worden beoordeeld hoe op bepaalde situaties wordt gereageerd (voorbeeld situatie: een ICT gerelateerd probleem doet zich voor op de werkvloer, zoals een virus uitbraak) en hoe personen handelen op dat moment.
- Literatuuronderzoek:
  - Raadplegen van (wetenschappelijke)artikelen, boeken en relevante websites welke antwoord kunnen geven op de onderzoeksvragen (en uiteindelijk bijdragen aan het beantwoorden van de hoofdvraag).
- Analyseren documentatie:
  - Mogelijk beschikt de organisatie over documentatie welke zij beschikbaar stelt zodat eventueel bruikbare inhoud (welke van belang kan zijn voor het onderzoek) kan worden toegepast in de opdracht.

3.5 Theoretisch kader

Er wordt gebruik gemaakt van de volgende theoretische onderwerpen betreffende de uitvoering van het project, welke een hulpmiddel kunnen zijn bij het beantwoorden van de hoofdvraag.

Standaarden

Gedurende de uitvoering van het project kan gebruik worden gemaakt van de volgende standaarden (welke bijv. bruikbare richtlijnen kunnen bevatten) wat betreft het uitvoeren van een risicoanalyse en het opstellen van een DRP. Mogelijke standaarden die hierbij kunnen worden geraadpleegd zijn o.a.:

- NIST 800-30 (2012) *Guide for Conducting Risk Assessments*, van het US National Institute for Standards and Technology (NIST). Standaard welke als leidraad kan fungeren voor organisaties m.b.t het uitvoeren van een risicoanalyse(NIST, 2012).
- NIST 800-34 (2010) *Contingency Planning Guide for Federal Information Systems*, van het US National Institute for Standards and Technology (NIST). Omschrijft een proces in stappen wat betreft de invoering van Business Continuity Planning en Disaster Recovery Planning projecten (NIST, 2010).
- ISO/IEC 24762:2008 (2008). *Guidelines for information and communications technology disaster recovery services*. Geeft richtlijnen voor het verstrekken van informatie en Disaster Recovery diensten (ISO/IEC 24762:2008, 2008).

- ISO/IEC 27031:2011 (2011). *Guidelines for information and communication technology readiness for business continuity*. Beschrijft o.a. de concepten en principes op het gebied van ICT m.b.t. de gereedheid voor business continuity (ISO/IEC 27031:2011, 2011).

Boeken

Wat betreft informatie omtrent het uitvoeren van een risicoanalyse en de opbouw van een DRP kunnen mogelijk de onderstaande boeken worden geraadpleegd:

- Snedaker, S. & Rima, C. (2014). *Business Continuity and Disaster Recovery Planning for IT Professionals.* ISBN: 9780124105263.
- Thejendra, B.S. (2014). *Disaster Recovery and Business Continuity*. (3rd ed.). ISBN: 9781849285384.
- Watters, J. (2014). *Disaster Recovery, Crisis Response and Business Continuity*. ISBN: 9781430264064.
- Blokdijk, G. (2012). Disaster Recovery 100 Success Secrets. (eBook).

Onderstaande boeken kunnen worden geraadpleegd m.b.t. het verrichten van onderzoek, voor het schrijven van rapporten en de scriptie:

- Steehouder, M. (2006). *Leren Communiceren* (5e Herz. ed.). ISBN: 9789001547028.
- Kiewiet-Kester, J. (2014). *Van werkdocument tot eindverslag*. ISBN: 9789046903766.
- Oosterbaan, W. (2014). *Een leesbare scriptie*. ISBN: 9789035142183.

Websites

Het internet biedt vele mogelijkheden om antwoorden te vinden op een groot aantal vraagstukken. Daarnaast worden op het internet ook geregeld interessante (wetenschappelijke) artikelen gepubliceerd waaruit nuttige informatie kan worden gewonnen. Omdat het hierbij belangrijk is dat kan worden gegarandeerd dat deze bronnen van het internet betrouwbaar zijn, dient te wordt gezocht op websites welke erom bekend staan betrouwbare informatie te bevatten. De volgende websites kunnen hiervoor mogelijk worden gebruikt:

- http://searchdisasterrecovery.techtarget.com/;
- scholar.google.nl;
- http://www.drj.com/;
- www.scientificpapers.org;
- gartner.com;
- http://dl.acm.org/.

Webinars

Tot slot kan ook veel nuttige informatie worden gewonnen uit het volgen van (recente) webinars. Hierin worden o.a. relevante onderwerpen besproken (bijv. op het gebied van Disaster Recovery):

- www2.agilityrecovery.com/education/;
- www.brighttalk.com.

3.5.1 Begrippen

Om duidelijkheid te verschaffen over de (kern)begrippen die tijdens het onderzoek en de uitvoering van het project worden gebruikt, zijn deze in onderstaande tabel beschreven:

Begrip	Definitie
Disaster Recovery plan (DRP)	Omschrijft het herstel van de business continuïteit, de primaire bedrijfsprocessen met inbegrip van de ICT apparatuur, wanneer een calamiteit heeft plaatsgevonden binnen een organisatie.
(Disaster) Recovery Strategy	Door de organisatie gekozen maatregelen om de primaire bedrijfsprocessen en bedrijfskritische ICT systemen na een calamiteit te herstellen.
Business Recovery Team (BRT)	Een groep personen die verantwoordelijk zijn voor de handhaving van het

	Disaster Recovery plan en Disaster Recovery strategieën (de coördinatie van het herstel van de primaire bedrijfsprocessen en bedrijfskritische systemen). Wordt ook wel een Disaster Recovery Team (DRT) genoemd.
Risk Analysis (Risicoanalyse)	Methode waarin mogelijke calamiteiten (gebeurtenissen of situaties) worden geïdentificeerd, een schatting wordt gemaakt van de waarschijnlijkheid dat de gebeurtenis zal plaatsvinden met kwalitatieve/ kwantitatieve resultaten om (m.b.v. prioriteren van primaire bedrijfsprocessen) de impact voor een organisatie te minimaliseren.
Asset	Een onderdeel welke de organisatie als belangrijk beschouwt binnen de bedrijfsvoering (zoals bedrijfsmiddelen, ICT apparatuur, imago etc.).

3.5.2 Beantwoording van de deelvragen

1. Hoe verlopen de primaire bedrijfsprocessen binnen de organisatie?		
Onderzoeksmethoden	**Onderzoeksfunctie**	**Begrippen**
• (Groeps)gesprekken/ Interviews • Analyseren documentatie	Beschrijven	Asset
Door gesprekken te voeren met de betrokken partijen (bedrijfsbegeleider, collega's) kunnen de primaire bedrijfsprocessen in kaart worden gebracht. Daarnaast kan eventueel middels beschikbaar gestelde documentatie door de organisatie meer informatie worden verkregen over deze primaire bedrijfsprocessen (eventuele websites die hierbij ook geraadpleegd zouden kunnen worden, bijv. wat betreft het overzichtelijk in kaart brengen van deze bedrijfsprocessen, zijn o.a. http://searchdisasterrecovery.techtarget.com/ en http://www.drj.com/).		
2. Welke bedrijfskritische systemen/ componenten zijn betrokken bij de primaire bedrijfsprocessen?		
Onderzoeksmethoden	**Onderzoeksfunctie**	**Begrippen**
• (Groeps)gesprekken/ Interviews • Analyseren documentatie	Beschrijven	Asset
Middels het voeren van gesprekken met de betrokken partijen wordt bepaald welke bedrijfskritische systemen/ componenten betrokken zijn bij de primaire bedrijfsprocessen. Op deze manier kan worden bepaald welke ICT systemen/ componenten vereist zijn bij het operationeel houden van de primaire bedrijfsprocessen binnen de organisatie. Hierbij zullen ook de specificaties van de bedrijfskritische systemen/ componenten in kaart worden gebracht. Daarnaast kan eventueel beschikbaar gestelde documentatie worden geraadpleegd, welke bijv. inzicht kan geven in de inrichting van de bedrijfsprocessen met de bijbehorende ICT systemen/ componenten.		
3. Welke ICT gerelateerde calamiteiten vormen een risico voor de bedrijfskritische systemen/ componenten?		
Onderzoeksmethoden	**Onderzoeksfunctie**	**Begrippen**
• Literatuur onderzoek • (Groeps)gesprekken/ Interviews	Verklaren	Risk Analysis Asset
Wanneer de primaire bedrijfsprocessen en bedrijfskritische systemen in kaart zijn gebracht, kan worden gestart met de Risicoanalyse. Hierbij is het belangrijk te weten welke mogelijke calamiteiten zich kunnen voordoen binnen de organisatie. Door middel van het bestuderen van literatuur kan informatie worden verkregen over de mogelijke calamiteiten die zoal kunnen optreden binnen organisaties en hoe vervolgens een Risicoanalyse kan worden gedefinieerd. Een standaard die kan worden geraadpleegd m.b.t. het uitvoeren van een risicoanalyse is "NIST (800-30). *Guide for Conducting Risk Assessments*". Het volgende boek kan hierbij ook worden gebruikt: "*Business Continuity and Disaster Recovery Planning for IT Professionals.* Snedaker, S. (2014)". De volgende websites kunnen ook veel informatie geven over deze onderwerpen, zoals http://www.drj.com/, http://searchdisasterrecovery.techtarget.com/ of www.brighttalk.com. Vervolgens kan in een gesprek (of interview) met de betrokken partijen binnen de organisatie worden bepaald welke calamiteiten zij relevant achten voor hun organisatie en hoe de kans/ impact/ prioriteiten kunnen worden ingeschat.		
4. Wat is de impact van de risico's op de bedrijfskritische systemen/ componenten en dus op de primaire bedrijfsprocessen?		
Onderzoeksmethoden	**Onderzoeksfunctie**	**Begrippen**
• (Groeps)gesprekken/ Interviews	Verklaren	Risk Analysis Asset

Wanneer de mogelijke calamiteiten in kaart zijn gebracht, kan met name aan de hand van gesprekken (interviews) met de betrokken partijen worden bepaald wat de kans en impact is van deze risico's op de primaire bedrijfsprocessen.

5. Welke maatregelen dienen genomen te worden om het risico op calamiteiten te verminderen en waar mogelijk te voorkomen?

Onderzoeksmethoden	Onderzoeksfunctie	Begrippen
• Literatuur onderzoek • (Groeps)gesprekken/ Interviews • Observeren	Ontwerpen	Risk Analysis (Disaster) Recovery Strategy Disaster Recovery plan (DRP)

Wanneer de risico's in kaart zijn gebracht kunnen maatregelen worden opgesteld om de risico's op calamiteiten te minimaliseren en waar mogelijk te voorkomen. Middels gesprekken met de betrokken partijen, en eventueel observatie, kan worden bepaald welke maatregelen er genomen kunnen worden binnen de organisatie wanneer calamiteiten zich voordoen. Ook middels literatuuronderzoek kan worden onderzocht hoe dit aangepakt kan worden, waarbij de volgende boeken geraadpleegd kunnen worden: "*Disaster Recovery, Crisis Response and Business Continuity*. Watters, J. (2014)" en "*Business Continuity and Disaster Recovery Planning for IT Professionals.* Snedaker, S. (2014)". Het internet kan ook meer duidelijkheid verschaffen over mogelijk te nemen maatregelen (bijv. op http://searchdisasterrecovery.techtarget.com/). Een mogelijke standaard die ook hierbij geraadpleegd kan worden is "NIST 800-34 (2010). *Contingency Planning Guide for Federal Information Systems*, van het US National Institute for Standards and Technology (NIST)".

6. Hoe dienen de verantwoordelijken binnen de organisatie te handelen in het geval van een calamiteit?

Onderzoeksmethoden	Onderzoeksfunctie	Begrippen
• Literatuur onderzoek • (Groeps)gesprekken/ Interviews	Ontwerpen	Disaster Recovery plan (DRP) Business Recovery Team (BRT)

Aan de hand van de gedefinieerde maatregelen, kunnen gesprekken worden georganiseerd zodat met de betrokken partijen (en o.a. de verantwoordelijke personen) kan worden besproken wat de juiste handelswijze is in het geval van een calamiteit. In de literatuur kan ook worden gezocht naar informatie wat betreft de mogelijkheden hoe calamiteiten kunnen worden aangepakt. Mogelijke boeken die hierbij kunnen worden geraadpleegd zijn o.a. "*Disaster Recovery, Crisis Response and Business Continuity*. Watters, J. (2014)" en "*Business Continuity and Disaster Recovery Planning for IT Professionals.* Snedaker, S. (2014)".

4. Projectactiviteiten

In dit hoofdstuk worden de projectactiviteiten uiteen gezet, welke zullen worden doorlopen gedurende de uitvoering van het project.

4.1 Fasering

4.1.1 Initiatie

De startfase van het project. In deze fase zal onder meer het Plan van Aanpak (PvA) worden gerealiseerd. Na goedkeuring van het PvA wordt vervolgens het Afstudeercontract opgesteld en ondertekend door de betrokken partijen. Daarnaast zal er binnen deze fase ook (voor)onderzoek worden verricht hoe een passende risicoanalyse (bijv. met welke technieken, standaarden) kan worden uitgevoerd en hoe uiteindelijk een DRP kan worden gedefinieerd. Het voornaamste doel van dit vooronderzoek is dat de organisatie een helder beeld krijgt wat een DRP eigenlijk inhoudt en hoe deze kan worden afgestemd op de organisatie in kwestie.

4.1.2 Analyse (Proces analyse en IT componenten analyse)

Wanneer het vooronderzoek is afgerond, kan in deze fase zal er worden gestart met het in kaart brengen van de primaire bedrijfsprocessen (de proces analyse) en bijbehorende bedrijfskritische systemen die deze processen ondersteunen (de IT componenten analyse).

4.1.3 Risicoanalyse

Wanneer de primaire bedrijfsprocessen met de bijbehorende ICT systemen in kaart zijn gebracht, zal worden gestart met een risicoanalyse. Op basis van de risicoanalyse kunnen vervolgens risico beperkende (en waar mogelijk preventieve) maatregelen worden gedefinieerd.

4.1.4 Disaster Recovery plan (DRP)

Tijdens deze fase wordt gestart met het opstellen van het Disaster Recovery plan. Daarnaast zal er ook een adviesrapport (waarvan het DRP onderdeel uit zal maken) worden opgeleverd die de organisatie voorziet van een passend advies met bijbehorende aanbevelingen betreffende het opvolgen van het DRP.

4.2 Project risico's

Met betrekking tot de uitvoering van deze opdracht verwacht de organisatie geen (grote) risico's. Het is echter niet uit te sluiten dat er gedurende het project risico's kunnen optreden die het succesvol slagen van de opdracht mogelijk in gevaar kunnen brengen. Deze risico's zijn onder meer:

- De omvang van de onderzoeksopdracht neemt dermate grote proporties aan dat de realisatie van het DRP niet haalbaar blijkt te zijn binnen de overeengekomen tijdspanne.
    - *Maatregel: wanneer blijkt dat de omvang van het project in strijd is met de overeengekomen tijdspanne, kan middels een overleg met de betrokken partijen (bedrijfsbegeleider, directie, docentbegeleider) worden bepaald of het project moet worden bijgesteld (bijv. omdat er in dit geval wordt afgeweken van het PvA, het project herzien zodat middels enige aanpassingen het project passend gemaakt kan worden binnen de tijd, zodat er alsnog een bruikbaar product wordt opgeleverd welke voldoet aan de eisen en wensen van zowel de organisatie als de opleiding).*
- Betrouwbaarheid waarborgen van de gebruikte onderzoeksbronnen.
    - *Maatregel: door gebruik te maken van goed onderbouwde en herleidbare informatiebronnen (zoals wetenschappelijke artikelen en informatie uit boeken), wordt de betrouwbaarheid van deze bronnen gewaarborgd.*
- Leveranciers zijn niet beschikbaar of product kan niet worden geleverd.
    - *Maatregel: wanneer een leverancier van de organisatie niet beschikbaar is voor bijv. vragen of wanneer een leverancier een specifiek product niet (meer) kan leveren, is het mogelijk dat een andere leverancier (die soortgelijke producten levert) kan worden geraadpleegd die de organisatie in deze behoefte kan voorzien.*
- De kwaliteit van het project voldoet niet aan de verwachtingen van de organisatie.
    - *Maatregel: door tussenopleveringen in te plannen en de resultaten te bespreken met de bedrijfsbegeleider (en evt. andere betrokkenen) kan worden beoordeeld of het project nog voldoet aan de verwachtingen van de organisatie.*

4.3 Communicatie

4.3.1 Organisatie

Om de kwaliteit van het project te garanderen, zijn er met de bedrijfsbegeleider wekelijkse terugkoppelingen gepland m.b.t. de uitvoering van de opdracht. Het is hierbij belangrijk dat aan de orde komt wat de voortgang is van het project (of er bijv. knelpunten zijn) en of het project nog voldoet aan de verwachtingen (kwaliteitsbewaking). Eventuele problemen die het slagen van de opdracht in gevaar kunnen brengen worden op deze manier tijdig aan het licht gebracht zodat ze vervolgens snel kunnen worden opgelost. Er is hierin ook ruimte voor feedback die het project in de goede richting kunnen sturen.

4.3.2 Opleiding

De docentbegeleider van de opleiding zal om de twee weken worden ingelicht over de voortgang van het project. M.b.t. de oplevering van eindproducten (zoals het adviesrapport en de scriptie), kan het voorkomen dat er frequenter zal worden gerapporteerd wat de status is (mede om de kwaliteit van deze producten te waarborgen). De student zal de docentbegeleider op eigen initiatief verzoeken feedback te geven op deze documentatie.

5. Randvoorwaarden

In dit hoofdstuk worden de (rand)voorwaarden m.b.t. het project omschreven. Hierbij volgt tot slot nog een beschrijving van de afbakening van het project.

Het afstudeerproject zal starten in september 2015 en eindigen in december 2015, **waarbij het project op 4 december 2015 dient te zijn afgerond**. Daarna zal in januari 2016 een afstudeerzitting worden ingepland om het afstudeerproject af te sluiten met een presentatie en een zitting.

5.1 Organisatorische randvoorwaarden

Met betrekking tot het afstudeerproject zijn er een aantal voorwaarden van toepassing:

Beschikbaarheid bedrijfsbegeleider

Gedurende het afstudeerproject is het belangrijk dat de bedrijfsbegeleider bereikbaar is op de momenten dat ondersteuning m.b.t. de uitvoer van de opdracht vereist is. Wanneer de bedrijfsbegeleider niet aanwezig is, neemt de kans toe dat het afstudeertraject 'niet meer te controleren is'. Toch kan het voorkomen dat de bedrijfsbegeleider (voor langere tijd) afwezig is, hiervoor dient een tweede begeleider aanwezig te zijn binnen de organisatie die de student kan ondersteunen in het afstudeertraject.

Beschikbaarheid docentbegeleider

Het is van belang dat de docentbegeleider te bereiken is in het geval feedback vereist is, of wanneer er dringende vragen m.b.t. het afstudeertraject beantwoord dienen te worden. Hierbij is een snelle terugkoppeling (bijv. in de vorm van passende feedback) op ingezonden documentatiestukken belangrijk, om vertraging van de uitvoer van het project te voorkomen. Dit dient echter door de student wel duidelijk aangegeven te worden wanneer hiervoor een verzoek wordt ingediend bij de docentbegeleider.

Beschikbaarheid collega's en leveranciers

Gedurende de uitvoer van het project dienen zowel collega's als leveranciers beschikbaar te zijn voor eventuele vragen, interviews of benodigde gegevens wanneer dit nodig is. Indien dit niet het geval is, kan er mogelijk geen antwoord worden gegeven op onderzoeksvragen en- of componenten die van cruciaal belang zijn voor de afronding van de eindproducten.

Beschikbaarheid van hard- en software

Om de afstudeeropdracht uit te voeren is het noodzakelijk dat hardware (zoals toegang tot de server ruimte wanneer dat nodig is) en software (zoals het Microsoft Office pakket voor het schrijven van documentatie) beschikbaar worden gesteld. Indien deze niet beschikbaar zijn, kan de opdracht niet worden uitgevoerd.

5.2 Afbakening

Dit afstudeerproject zal zich beperken tot de volgende aspecten:

- Het DRP dient een solide basis te vormen voor de organisatie betreffende de handelswijze (de te nemen maatregelen) in geval van calamiteiten. Het testen van het DRP wordt niet meegenomen in dit project.
- Het DRP zal zich richten op de ICT systemen/ componenten die zijn betrokken bij de primaire bedrijfsprocessen (welke uiteindelijk zorg dragen voor de continuïteit van de organisatie).
- M.b.t. de uitvoering van het project en het DRP worden alleen de calamiteiten onderzocht welke hun oorzaak hebben in de ICT systemen en dus op de continuïteit van de primaire bedrijfsprocessen (bijv. calamiteiten zoals hardware falen en diefstal van IT gegevens). Calamiteiten welke gevolgen hebben voor de ICT systemen, zoals een brand in de server ruimte, worden ook meegenomen in het project. Overige calamiteiten die geen invloed hebben op de ICT omgeving zullen niet worden meegenomen in het project (bijv. calamiteiten zoals schade aan het bedrijfspand of brand in een vergaderzaal).
- Het contractuele/ wettelijke aspect zal niet worden meegenomen in dit project, omdat er binnen de organisatie nog geen regelgeving aanwezig is op gebied van ICT (waaruit bijv. blijkt dat de organisatie moet voldoen aan een bepaalde contractuele regels/eisen wat betreft de ICT omgeving). In de toekomst

verwacht de organisatie echter te groeien waardoor zij moeten voldoen aan strengere eisen. Hierdoor moet de organisatie op lange termijn wel beschikken over een bepaalde regelgeving (en dus ook op gebied van de ICT), maar dat blijft voor dit project buiten beschouwing.

6. Projectplanning

In 'Figuur 1, Projectplanning' is een globale projectplanning opgenomen met daarbij de geschatte uren. De planning zal regelmatig worden geraadpleegd gedurende de uitvoering van het project, om te controleren of de projectactiviteiten nog verlopen volgens schema. Wanneer nodig, zal in overleg de planning worden bijgestuurd.

Maand	Activiteit	Datum van	Datum tot	Uren
Augustus	Startsessie #1 Afstudeerleerteam	25/8/2015	25/8/2015	[8]
	Start Afstudeerstage Tsubakimoto	**31/8/2015**	**22/1/2016**	**840**
September	**Start "Initiatie fase"**	**31/8/2015**	**30/9/2015**	**180**
	Werken aan realisatie PvA	31/8/2015	30/9/2015	[80]
	Verrichten vooronderzoek project	31/8/2015	30/9/2015	[100]
	PvA sessie #2 Afstudeerleerteam	23/9/2015	23/9/2015	[8]
	Bezoek docentbegeleider organisatie	*30/9/2015*	*30/9/2015*	
Oktober	**Start "Analyse fase"**	**1/10/2015**	**15/10/2015**	**90**
	> Beantwoorden deelvraag 1			[40]
	> Beantwoorden deelvraag 2			[40]
	Werken aan realisatie Adviesrapport	1/10/2015	4/12/2015	**100**
	Werken aan realisatie Scriptie	1/10/2015	15/12/2015	**130**
	Uiterlijke inleverdatum Afstudeercontract	15/10/2015	15/10/2015	
	Inleveren Scriptie (concept 1)	23/10/2015	23/10/2015	
	Scriptiesessie #3 Afstudeerleerteam	28/10/2015	28/10/2015	[8]
	Start "Risicoanalyse fase"	**16/10/2015**	**30/10/2015**	**90**
	> Beantwoorden deelvraag 3			[40]
	> Beantwoorden deelvraag 4			[40]
November	**Start "Disaster Recovery plan (DRP) fase"**	**2/11/2015**	**30/11/2015**	**170**
	> Beantwoorden deelvraag 5			[40]
	> Beantwoorden deelvraag 6			[40]
	Inleveren Scriptie (concept 2)	20/11/2015	20/11/2015	
	Opleveren Disaster Recovery plan (DRP)	30/11/2015	30/11/2015	
December	Opleveren Adviesrapport	4/12/2015	4/12/2015	
	Einddatum Project	***4/12/2015***	***4/12/2015***	
	Mogelijke uitloop project	*7/12/2015*	*14/12/2015*	
	Uiterlijke inleverdatum Scriptie	15/12/2015	15/12/2015	
Januari	Voorbereiding Afstudeerpresentatie	16-12-2015	22/1/2016	**80**
	Afstudeerpresentatie (en zitting)	*14/1/2016*	*22/1/2016*	
	Exacte data volgen nog!			

Figuur 1. Projectplanning

7. Persoonsgegevens

Onderwijsinstelling

Adres: Hogeschool Utrecht
Nijenoord 1
3552 AS Utrecht
Telefoon: 088 481 8283

Docentbegeleider: Dhr. L. M. Roeleveld
E-mail: leen.roeleveld@hu.nl

Student: Mirthe van de Wildenberg
Opleiding: System and Network Engineering
Studentnummer: 1610609
Telefoon: 06 10 414 353
E-mail (persoonlijk): wildenberg.mirthe@gmail.com
E-mail (student): mirthe.vandewildenberg@student.hu.nl

Organisatie

Adres: Tsubakimoto Europe B.V.
Aventurijn 1200
3316 LB Dordrecht
Telefoon: 078 620 4000
E-mail: info@tsubaki.eu
Website: www.tsubaki.eu

Bedrijfsbegeleider: Dhr. C. Bruntink
Functie: ICT Manager
Telefoon: 06 20 709 362
E-mail: cor.bruntink@tsubaki.eu

8. Bronvermelding

ISO/IEC 24762:2008. (2008). Geraadpleegd op 9 september 2015, op http://www.iso.org/iso/catalogue_detail?csnumber=41532

ISO/IEC 27031:2011. (2011). Geraadpleegd op 9 september 2015, op http://www.iso.org/iso/catalogue_detail?csnumber=44374

Kiewiet-Kester, J. (2014). *Van werkdocument tot eindverslag*. Bussum: Coutinho.

MoSCoW-methode. (z.d.). Geraadpleegd op 4 september 2015, op http://www.marketingtermen.nl/begrip/moscow-methode

NIST. (2012). *Guide for Conducting Risk Assessments* (NIST Special Publication 800-30 Rev. 1). Gedownload op 21 september 2015, op http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Snedaker, S. & Rima, C. (2013). *Business Continuity and Disaster Recovery Planning for IT Professionals*. Waltham, MA: Syngress

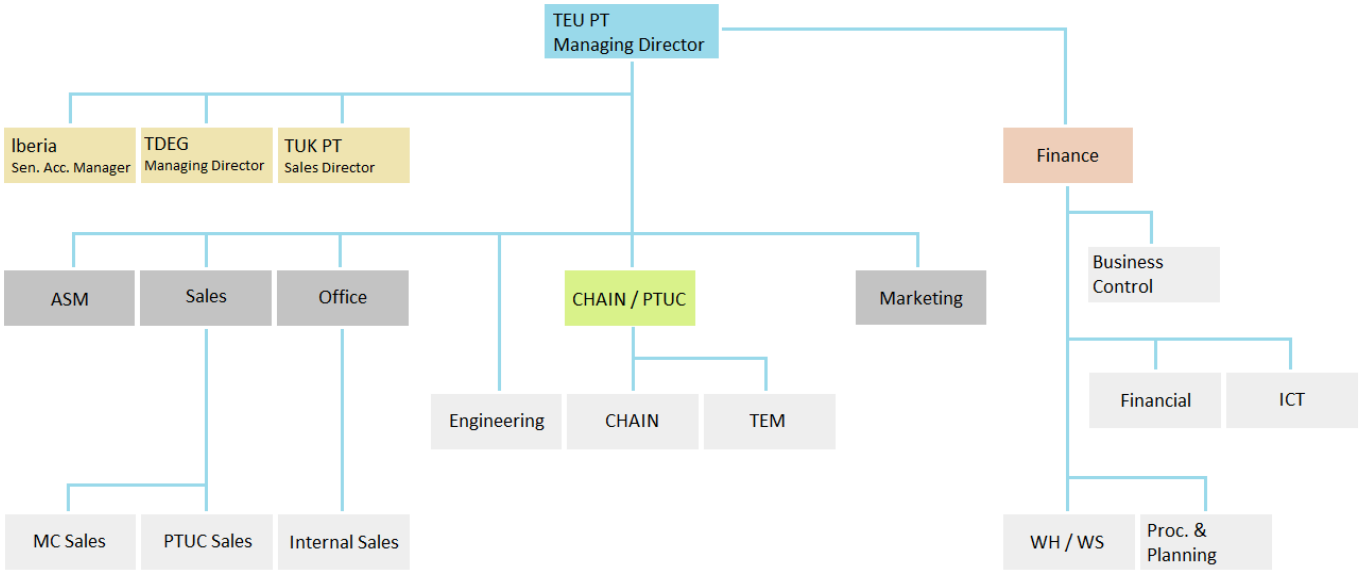
Swanson, M., Bowen, P., Wohl-Philips, A., Gallup, D., & Lynes, D. (2010). *Contingency Planning Guide for Federal Information Systems* (NIST Special Publication 800-34 Rev. 1). Gedownload op 9 september 2015, op http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Taalwinkel. (z.d.). Afstuderen Stap 1: Onderzoeksmethoden kiezen. Geraadpleegd op 8 september 2015, op http://www.taalwinkel.nl/tekstsoorten/onderzoeksmethoden-kiezen/

Tsubakimoto Europe B.V. (2015). Geraadpleegd op 4 september 2015, op http://tsubaki.eu/

Tsubakimoto Europe B.V. (2015). *Power Transmission Management Organisation Chart*.

Bijlage 1: Organigram Tsubakimoto Europe B.V.



Figuur 2. Organigram Tsubakimoto Europe B.V. Bewerkt van "Power Transmission Management Organisation Chart," (Tsubakimoto Europe B.V., 2015).

Afkortingenlijst			
TEU PT	Tsubaki Europe Power Transmission	TEM	Tsubaki Emerson
TDEG	Tsubaki Deutschland GmbH	MC Sales	Motorcycle Chain Sales
TUK PT	Tsubaki United Kingdom Power Transmission	PTUC Sales	Power Transmission Unit Components Sales
ASM	Area Sales Manager	WH / WS	Warehouse / Workshop
PTUC	Power Transmission Unit Components	Proc. & Planning	Procurement & Planning

Bijlage 2: Afdeling omschrijving

De organisatie beschikt over de volgende afdelingen met daarbij de belangrijkste taken:

Afdeling	Omschrijving
Engineering	• Verbeteren technische competenties m.b.t. producten, ondersteunen verkoop.
Finance & Control	• Financiele administratie, • Monitoring risico management, • Monitoring strategische financiele positie TEU Group.
Internal Sales	• Verantwoordelijk voor interne/ externe communicatie, • Correcte verwerking van administratie, • Controle bestellingen.
ICT	• Monitoring/managen IT budget, • Monitoring/managen dagelijkse IT werkzaamheden, • Onderhouden/ondersteunen (interne) infrastructuur en gebruikers.
Marketing	• Ondersteunen projectteams, • Monitoring/onderhouden marketing budget, • Verbeteren kansen op de markt, • Ontwikkelen promotie activiteiten, • Verkoop communicatie.
MC Sales	• Bijdrage leveren verkoopbeleid, verkoopproces, • Verhogen omzet organisatie (bijdrage algemene tevredenheid klant t.o.v. werkgevers, prijs, reactiesnelheid).
Procurement & Planning	• Afwerking inkooporders en contacten met leveranciers, • Beheren van Sales Contracts, • Follow-up leveranciers voor op tijd leveren.
TEM-EU	• Sales (bijdrage leveren verkoopbeleid, verkoopproces, verhogen omzet organisatie), bijdragen algemene tevredenheid klant t.o.v. werkgevers, prijs, reactiesnelheid.
Warehouse/Workshop	• Monitoring/aansturen activiteiten operationele afdeling, werkplaats, magazijn, • Inruimen ontvangen goederen, verzendklaar maken producten, • Inplannen werkzaamheden Workshop, • Verwerken van in- en uitgaande goederen, • Assembleren en bewerken van producten.

Bijlage 3: Afstudeercontract

BIJLAGE 5

Contract afstudeeropdracht
Institute for ICT
Nijenoord 1, 3552 AS, UTRECHT

Naam student : Mirthe vd Wildenberg

Afstudeerrichting: System and Network Engin. Variant: voltijd / ~~deeltijd~~ / ~~duaal~~

Adres student : Dieselstraat 74

Postcode / Woonplaats student: 3112 KC, Schiedam

Studentnummer : 1610609

Telefoonnummer privé : 06 10 414 353

E-mailadres : Mirthe.vandewildenberg@student.hu.nl
wildenberg.mirthe@gmail.com

Naam bedrijf (afstuderen) : Tsubakimoto Europe B.V.

Adres bedrijf : Aventurijn 1200

Postcode / Woonplaats bedrijf : 3316 LB, Dordrecht

Naam bedrijfsbegeleider : Dhr. Cor Bruntink

Telefoonnummer bedrijfsbegeleider : 06 20 709 362

E-mailadres bedrijfsbegeleider : cor.bruntink@tsubaki.eu

Beoogde maand van afstuderen : Januari 2016 *maand en jaar invullen*

Geheimhouding geaccordeerd door HU op : *indien van toepassing*

Inleverdata van twee concept-scripties : 23-10-2015 / 20-11-2015

Beschrijving van de afstudeeropdracht

Geef hier in enkele zinnen weer wat de afstudeeropdracht inhoudt.

De opdracht omvat het onderzoeken van de te nemen maatregelen om risico's op ICT gerelateerde calamiteiten te minimaliseren en waar mogelijk te voorkomen. Daarnaast wordt ook onderzocht hoe de verantwoordelijken dienen in te grijpen in het geval van een calamiteit. (Deze aspecten zullen uiteindelijk worden opgenomen in de realisatie van het Disaster Recovery Plan).

Hoofd- een deelvragen van het uit te voeren onderzoek

Noteer hier de hoofdvraag met deelvragen van het onderzoek dat voor het uitvoeren van de afstudeeropdracht moeten worden uitgevoerd.

→ Hoofdvraag: "Welke maatregelen zijn noodzakelijk om enerzijds het risico op calamiteiten te minimaliseren en anderzijds adequaat in te grijpen bij calamiteiten?"
- Hoe verlopen de primaire bedrijfsprocessen binnen de organisatie?
- Welke bedrijfskritische systemen/componenten zijn betrokken bij de primaire bedrijfsprocessen?
- Welke ICT gerelateerde calamiteiten vormen een risico voor de bedrijfskritische systemen/componenten?
- Wat is de impact van de risico's op de bedrijfskritische systemen/componenten en dus op de primaire bedrijfsprocessen?
- Welke maatregelen dienen genomen te worden om het risico op calamiteiten te verminderen en waar mogelijk te voorkomen?
- Hoe dienen de verantwoordelijken binnen de organisatie te handelen in het geval van een calamiteit?

Op te leveren producten

Beschrijf hier de producten die aan het einde van het afstudeerproject moeten zijn opgeleverd.

Deelproducten:
- Vooronderzoek
- procesanalyse & IT Componenten analyse
- Risico analyse

Eindproducten:
- Disaster Recovery Plan
- Adviesrapport
- Scriptie

-43-

Akkoordverklaringen

Ondergetekenden verklaren akkoord te gaan met de afstudeeropdracht, de hoofd- en deelvragen van het uit te voeren onderzoek en de op te leveren producten zoals hiervoor beschreven.
Bovendien verklaren zij dat op basis van deze gegevens door de student een plan van aanpak is geschreven dat door betrokkenen is goedgekeurd.

Handtekeningen

Datum : 12-10-2015

Student :

Docentbegeleider

Bedrijfsbegeleider[9]

[9] Door ondertekening van dit formulier verklaart de bedrijfsbegeleider (en eventuele mede-begeleiders) over voldoende kennis te beschikken, op minimaal HBO-niveau, om de afstudeerder te begeleiden.

Bijlage B - Berekeningen risicoanalyse

Brand

Fire	*IT equipment (and therefore, data) may be lost in case of a fire.*	0,0001	€ 180.000,00	€ 18,00
	Collateral damage: smoke/ soot damage which might cause damaged or loss of IT equipment (and therefore, data).	0,0001	€ 180.000,00	€ 18,00

Uit gegevens van het Centraal Bureau voor de Statistiek (CBS) blijkt dat er in Nederland 218.830 bedrijven zijn die vallen onder de bedrijfstak Handel, waar Tsubakimoto tevens deel van uit maakt (CBS, 2015).

Op de website van het VEBON is een overzicht weergegeven van het aantal bedrijfsbranden in Nederland per jaar (van 2004 tot 2014). Hieruit is het gemiddelde aantal bedrijfsbranden per jaar berekend: 17 + 13 + 21 + 23 + 23 + 28 + 20 + 23 + 32 + 35 + 31 = 266. 266 / 11 = 24 (VEBON, 2014).

De kans op jaarbasis die hieruit is berekend is als volgt: **24 / 218.830 = 0,0001**

Om de kosten te berekenen is in overleg met de opdrachtgever uitgegaan van de volgende situatie:

- De hardware kosten bedragen totaal € 125.000,00 (uitgaande dat alle hardware hierbij verloren is gegaan);
- Er dient een week lang extern personeel ingehuurd te worden om de bedrijfsvoering te herstellen. Hierbij is een schatting gemaakt dat de kosten € 200,00 per persoon bedragen, per dag. Uitgaande dat er vijf personen ingehuurd dienen te worden, bedragen de totaal kosten per dag: 200 x 5 = € 1000,00. 1000 x 5 = € 5000,00 (om in een week de bedrijfsvoering te herstellen na een brand);
- Tsubakimoto beschikt over 50 werkplekken, en het uurloon bedraagt €25,00. Indien de bedrijfsvoering een uur lang stil ligt, bedraagt dit: 50 x 25 = € 1250,00 per uur. Een werkweek duurt 40 uur, dus wanneer de bedrijfsvoering een week lang stil ligt in het geval van een brand, bedragen de kosten: 40 x 1250 = € 50.000,00;
- Uitgaande dat het een week duurt om de bedrijfsvoering te herstellen, bedragen de kosten (impact): 125.000 + 5000 + 50.000 = € 180.000,00;
- Totaalkosten (risico) = 0,0001 (kans) x 180.000 (impact) = **€ 18,00**.

Waterschade

Water damage	*Leakage: heavy rain or leaking pipes, frost/thaw might cause damaged or loss of IT equipment (and therefore, data).*	0,001	€ 180.000,00	€ 180,00

Uit een rapport van de Ombudsman van de Verzekeringen, blijkt dat er 267 gevallen van waterschade zijn gemeld in het jaar 2014 (Ombudsman, 2014).

De kans op jaarbasis die hieruit is berekend is als volgt: **267 / 218.830 = 0,001**

Om de kosten te berekenen is in overleg met de opdrachtgever uitgegaan van de volgende situatie:

- De hardware kosten bedragen totaal € 125.000,00 (uitgaande dat alle hardware hierbij verloren is gegaan);
- Er dient een week lang extern personeel ingehuurd te worden om de bedrijfsvoering te herstellen. Hierbij is een schatting gemaakt dat de kosten € 200,00 per persoon bedragen, per dag. Uitgaande dat er vijf personen ingehuurd dienen te worden, bedragen de totaal kosten per dag: 200 x 5 = € 1000,00. 1000 x 5 = € 5000,00;
- Uitgaande dat de bedrijfsvoering een week lang stil ligt, bedragen de kosten: 1250 (totaalkosten van manuren per uur) x 40 (gehele werkweek) = € 50.000,00;
- De kosten bedragen (impact): 125.000 + 5000 + 50.000 = € 180.000,00;
- Totaalkosten (risico): 0,001 (kans) x 180.000 (impact) = **€ 180,00**.

Stroomuitval

Power outage	*Electrical storms or a short circuit in power supply may cause a power outage.*	0,08	€ 1250,00	€ 100,00

Uit een rapport ("Betrouwbaarheid van elektriciteitsnetten in Nederland Resultaten 2014", pagina 3) van Netbeheer Nederland blijkt dat er 17.757 meldingen zijn binnengekomen van stroomuitval (met onderbrekingen tot gevolg) in 2014 (Netbeheer, 2014).

De kans op jaarbasis die hieruit is berekend is als volgt: **17.757 / 218.830 = 0,08**

Om de kosten te berekenen is in overleg met de opdrachtgever uitgegaan van de volgende situatie:

- Uitgaande dat door een stroomstoring, de bedrijfsvoering voor 60 minuten stil ligt;
- De kosten bedragen (impact): 50 (aantal werkplekken) x 25 (uurloon) = € 1250,00 (totaalkosten van manuren per uur);
- Totaalkosten (risico) = 0,08 (kans) x 1250 (impact) = **€ 100,00**.

Virusaanval

Malware/ virus attacks	*Malware or viruses are capable of data deletion, destruction or manipulation (which also might cause data loss).*	2	€ 5000,00	€ 10.000,00

In overleg met de opdrachtgever is m.b.t. dit risico besloten uit te gaan van de 'eigen ervaringen' van de organisatie.

- In overleg met de opdrachtgever is gebleken dat **2** gevallen van virusaanvallen per jaar voorkomen, welke daadwerkelijk fysieke schade toebrengen aan bedrijfsdata;
- Uitgaande dat de bedrijfsvoering voor een halve dag stil ligt, bedragen de kosten (impact): 1250 (totaalkosten aan manuren per uur) x 4 (halve werkdag bedraagt vier uur) = € 5000,00;
- Totaalkosten (risico) = 2 (kans) x 5000 (impact) = **€ 10.000,00**.

Inbraak

Burglary	*Vandalism: damaged or loss of IT equipment (and therefore, data).*	0,2	€ 180.000,00	€ 36.000,00
	Theft: loss of IT equipment (and therefore, data).	0,2	€ 180.000,00	€ 36.000,00

In totaal zijn er 185 bedrijven op het industrieterrein De Dordtse Kil III, waar tevens Tsubakimoto is gevestigd (Vereniging beheer Dordtse Kil III, 2009). Er zijn in totaal 37 gevallen van bedrijfsinbraken gemeld in dit gebied (Interpolis, 2012).

De kans op jaarbasis die hieruit is berekend is als volgt: 37 / 185 = **0,2**

Om de kosten te berekenen is in overleg met de opdrachtgever uitgegaan van de volgende situatie:

- Uitgaande van vandalisme (beschadiging/ vernieling van IT systemen) en diefstal, van alle IT systemen, bedragen de kosten: € 125.000,00 (totaal aantal hardwarekosten);
- Er dient een week lang extern personeel ingehuurd te worden om de bedrijfsvoering te herstellen. Hierbij is een schatting gemaakt dat de kosten € 200,00 per persoon bedragen, per dag. Uitgaande dat er vijf personen ingehuurd dienen te worden, bedragen de totaal kosten per dag: 200 x 5 = € 1000,00. 1000 x 5 = € 5000,00;
- Uitgaande dat de bedrijfsvoering een week lang stil ligt, bedragen de kosten: 1250 (totaalkosten van manuren per uur) x 40 (gehele werkweek) = € 50.000,00;
- De kosten bedragen (impact): 125.000 + 5000 + 50.000 = € 180.000,00;
- Totaalkosten (risico) = 0,2 (kans) x 180.000 (impact) = **€ 36.000,00**.

Incidentele acties

Accidental actions	*Altering, deleting, destroying data (accidental deletion of data or accidental altering of data which also might cause data loss).*	10	€ 6,25	€ 62,50

In overleg met de opdrachtgever is m.b.t. dit risico besloten uit te gaan van de 'eigen ervaringen' van de organisatie.

- In overleg met de opdrachtgever is uitgegaan van **10** gevallen per jaar, waarbij personeelsleden bedrijfsdata per ongeluk aanpassen, verwijderen of vernietigen;
- Uitgaande dat er een kwartier benodigd is om de bestanden te herstellen, bedragen de kosten (impact): 25 (uurloon van een personeelslid) / 4 (60 minuten / 15 minuten = 4) = € 6,25;
- Totaalkosten (risico) = 10 (kans) x 6,25 (impact) = **€ 62,50**.

Hardware problemen/ falen

Hardware issues/ failure	*Loss of data.*	0,2	€ 50,00	€ 10,00
	Loss of network connectivity: (i.e. no access to the internet or e-mail).	2	€ 5000,00	€ 10.000,00
	Loss of IT equipment: (i.e. a defect in the hard disk which causes the system to crash).	0,2	€ 125.000,00	€ 25.000,00

Loss of data:
In overleg met de opdrachtgever is m.b.t. dit risico besloten uit te gaan van de 'eigen ervaringen' van de organisatie.

- In overleg met de opdrachtgever is gebleken dat er 3 gevallen van dataverlies (door hardware problemen) zijn voorgekomen in 15 jaar. De kans op jaarbasis bedraagt hierbij: 3 / 15 = **0,2**;
- Uitgaande dat het twee uur duurt om te herstellen van een dergelijke situatie, bedragen de kosten (impact): 25 (uurloon van een personeelslid) x 2 (aantal uren) = € 50,00;
- Totaalkosten (risico) = 0,2 (kans) x 50 (impact) = **€ 10,00**.

Loss of network connectivity:
In overleg met de opdrachtgever is m.b.t. dit risico besloten uit te gaan van de 'eigen ervaringen' van de organisatie.

- In overleg met de opdrachtgever is gebleken dat er **2** gevallen, van verlies van internetconnectiviteit, voorkomen per jaar;
- Uitgaande dat de bedrijfsvoering voor een halve dag stil ligt, bedragen de kosten (impact): 1250 (totaalkosten van manuren per uur) x 4 (halve werkdag bedraagt vier uur) = € 5000,00;
- Totaalkosten (risico) = 2 (kans) x 5000 (impact) = **€ 10.000,00**.

Loss of IT equipment:
In overleg met de opdrachtgever is m.b.t. dit risico besloten uit te gaan van de 'eigen ervaringen' van de organisatie.

- In overleg met de opdrachtgever is gebleken dat er 3 gevallen van verlies van apparatuur (door hardware problemen/ falen) zijn voorgekomen in 15 jaar. De kans op jaarbasis bedraagt hierbij: 3 / 15 = **0,2**;
- Uitgaande van totaal verlies van IT systemen, bedragen de kosten (impact): € 125.000,00;
- Totaalkosten (risico) = 0,2 (kans) x 125.000 (impact) = **€ 25.000,00**.

Falen leverancier

Vendor failure	*Loss of IT equipment (i.e. due to a fire at the vendor's location) – the (secondary) database server is hosted at an off-site location.*	0,0001	€ 6.000,00	€ 0,60

In overleg met de opdrachtgever is m.b.t. dit risico besloten uit te gaan van totaalverlies van de database server (welke zich bevindt binnen een extern datacenter van een leverancier) door brand.

- Uitgegaan van verlies van de (secundaire) database server door een brand bij de leverancier, kans = 0,0001;
- De kosten van de (secundaire) database server bedragen (impact): € 6000,00;
- Totaalkosten (risico) = 0,0001 (kans) x 6000 (impact) = **€ 0,60**.