Disaster Recovery planning

Appendix: 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: 10-12-2015

Inhoudsopgave

Bijlage 1 - Vooronderzoek

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).

Het ontbreken van een Disaster Recovery plan kan desastreuze gevolgen hebben voor organisaties (bijv. verantwoordelijken binnen de organisatie zijn niet op de hoogte hoe zij kunnen ingrijpen in geval van calamiteiten). Daarom is het voor Tsubakimoto Europe B.V. belangrijk te beschikken over een Disaster Recovery plan, zodat de verantwoordelijken binnen de organisatie weten welke passende maatregelen genomen moeten worden om te herstellen van calamiteiten binnen de ICT omgeving.

Dit vooronderzoek presenteert de belangrijkste resultaten en is verricht met als voornaamste doel inzicht te krijgen in Disaster Recovery planning (wat is disaster recovery planning?, wat is de inhoud van een disaster recovery plan?), en het uitvoeren van een risicoanalyse.

2. Disaster Recovery plan (DRP)

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).

2.1 Wat is een Disaster Recovery plan (DRP)?

Een Disaster Recovery plan omschrijft een gestructureerde aanpak om in te grijpen in het geval van calamiteiten binnen de IT infrastructuur (welke hardware, software, netwerken, processen en mensen omvat). Het belangrijkste doel van een Disaster Recovery plan is het formuleren van gedetailleerde herstel procedures, waarin de te ondernemen stappen worden omschreven die nodig zijn om IT systemen te herstellen naar een toestand waarin ze de organisatie na een calamiteit kunnen ondersteunen. (Kirvan, 2011).

2.2 Indeling Disaster Recovery plan[1]

Een Disaster Recovery plan omschrijft stapsgewijs de handelswijze in het geval van calamiteiten. De omschreven procedures dragen bij aan een eenvoudig toe te passen en herhaalbaar proces voor het herstellen van uitgevallen IT componenten en hoe deze zo snel mogelijk kunnen worden hervat (Kirvan, 2011).

Onderstaande opbouw van het Disaster Recovery plan is akomstig uit het boek: Business Continuity and Disaster Recovery Planning for IT professionals (Snedaker, 2014):

Activering

De activeringsfase bepaalt wanneer het Disaster Recovery plan wordt geactiveerd en op welke wijze. Het is voor organisaties niet wenselijk om een dergelijk plan voor elke kleine gebeurtenis te activeren. Er

[1] Raadpleeg http://searchdisasterrecovery.techtarget.com/feature/IT-disaster-recovery-DR-plan-template-A-free-download-and-guide voor een voorbeeld template van het Disaster Recovery plan

dient dus een duidelijke procedure beschikbaar te zijn die bepaalt wanneer het Disaster Recovery plan 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.

Onderhoud van het Disaster Recovery plan dient plaats te vinden ongeacht of het Disaster Recovery plan ooit is geraadpleegd. Het Disaster Recovery plan dient op een periodieke basis te worden herzien, om ervoor te zorgen dat het plan nog steeds actueel en relevant is voor de organisatie. Bijv. als operatieve of technologische wijzigingen zijn toegepast (zoals het wijzigen van locatie), moeten deze wijzigingen ook in het Disaster Recovery plan worden doorgevoerd.

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

Gedefinieerde rollen en verantwoordelijkheden per team, verduidelijken welke persoon bepaalde taken heeft te vervullen in het geval van een calamiteit. Benodigde gereedschappen en apparatuur dient hierbij ook in kaart te worden gebracht (bijv. beschikbaar stellen van brandblussers).

Communicatie
Wanneer er een incident plaatsvindt binnen de organisatie, moet er een proces zijn ontwikkeld om een incident te melden aan de teamleden. Dit gebeurt tevens als onderdeel van de Disaster Recovery plan activatie, en is een essentieel aspect dat duidelijk moet worden afgebakend. Hoe worden de teamleden op de hoogte gesteld? Welke processen, middelen en technologieën zijn hierbij nodig?

Er dient ook rekening gehouden te worden met de communicatie naar de overige personeelsleden die geen deel uitmaken van de activatie van het Disaster Recovery plan en herstel teams. Wanneer er calamiteiten optreden binnen de organisatie, moet er ook een procedure zijn om de personeelsleden op de hoogte te stellen van de situatie.

Herstelprocedures
Het nemen van (nood)maatregelen vloeit voort uit de risico's die zijn geïdentificeerd voor de organisatie. Deze maatregelen zijn de onmiddellijke reactie op een incident. Een eenvoudig herstelplan dat een verscheidenheid aan calamiteiten dekt zal helpen het herstelproces soepel te laten verlopen.

Logboek
Een logboek omvat in veel gevallen een beschrijving van de gebeurtenissen die hebben geleid tot een calamiteit en hoe een calamiteit is opgelost. Een logboek kan helpen de gebeurtenissen op papier te zetten en is een zeer nuttig proces om vast te leggen welke acties zijn ondernomen om een calamiteit in de toekomst te kunnen voorkomen.

3. Risicoanalyse

Het uitvoeren van een risicoanalyse omvat risico identificatie, inschatten van de kans van optreden en het definiëren van de ernst van de gevolgen. Het kan daarnaast ook nuttig zijn een 'vulnerability assessment' (kwetsbaarheid beoordeling) uit te voeren, zodat situaties die het risico op calamiteiten kunnen verhogen in kaart worden gebracht (Kirvan, 2010).

3.1 Begrippen en definities

3.1.1 Risk

Risico is een meting voor de mate waarin een entiteit wordt bedreigd door een potentiële omstandigheid of gebeurtenis, en is een functie van: (1) het nadelige effect (impact) dat ontstaat wanneer de omstandigheid of gebeurtenis plaatsvindt, en (2) de waarschijnlijkheid (probability) van optreden (NIST, 2012).

3.1.2 Threat

Een bedreiging is een omstandigheid of gebeurtenis met het potentieel om organisatorische activiteiten en activa, individuen of andere organisaties negatief te beïnvloeden d.m.v. een informatiesysteem via ongeautoriseerde toegang, vernietiging, verspreiding of wijziging van informatie (NIST, 2012).

3.1.3 Vulnerability

Een kwetsbaarheid is een zwakke plek in een informatiesysteem, beveiligingsprocedures of implementatie welke kan worden misbruikt door een bedreiging (NIST, 2012).

3.1.4 Likelihood

De kans (waarschijnlijkheid) is een gewogen risicofactor welke is gebaseerd op de waarschijnlijkheid dat een bepaalde bedreiging een kwetsbaarheid kan uitbuiten. De kans omvat de inschatting van de risico kans dat een bedreiging optreedt met een schatting van de impact wanneer deze bedreiging zich voordoet (NIST, 2012).

3.1.5 Impact

De impact is de omvang van de schade die kan worden verwacht welke het gevolg is van ongeautoriseerde bekendmaking, wijziging, vernietiging of verlies van gegevens, wanneer een bedreiging zich voordoet (NIST, 2012).

3.2 Methoden

3.2.1 Kwalitatief

Een kwalitatieve beoordeling maakt gebruik van woorden of relatieve waarden om risico, kosten en impact uit te drukken (Snedaker, 2014).Het bereik van een kwalitatieve risicobeoordeling is echter relatief klein in de meeste gevallen, wat het moeilijker maakt om de prioriteiten of vergelijkingen binnen de set van gerapporteerde risico's te definiëren. De herhaalbaarheid en reproduceerbaarheid van kwalitatieve risicobeoordelingen worden verhoogd wanneer de geëvalueerde waarden (per niveau) worden ondersteunt door zinvolle omschrijvingen (bijv. deze waarde is "hoog" wegens de volgende redenen...) en wanneer tabellen worden gebruikt om kwalitatieve waarden te combineren (NIST, 2012).

Likelihood	Description	Impact	Description
Rare	Once every 5 years	Very low	Negligible impact on continuity organization
Unlikely	Once every 2 years	Low	Minor impact on continuity organization
Moderate	Once every year	Medium	Significant impact on continuity organization
Likely	2 - 5 times a year	High	Serious impact on continuity organization

Common	More than 5 times a year	Very high	Critical impact on continuity organization

3.2.2 Kwantitatief

Een kwantitatieve beoordeling maakt gebruik van metingen en getallen. Ze zijn specifiek en meetbaar (Snedaker, 2014). De nauwkeurigheid van kwantificering wordt echter verminderd wanneer persoonlijke opvattingen zijn gemoeid met de kwantitatieve beoordeling, of wanneer m.b.t. de vaststelling van de waarden een mate van onzekerheid gepaard gaat. Een kwantitatieve beoordeling biedt echter ook het voordeel dat de resultaten exact, herhaalbaar en reproduceerbaar zijn vast te stellen (NIST, 2012).

Threat	Annual likelihood	Impact per incident	Risk cost
Threat 1	2	€ 1000	€ 2000
Threat 2	1	€ 500	€ 500
Threat 3	2	€ 10.000	€ 20.000
Threat 4	2	€ 1500	€ 3000
Threat 5	3	€ 2000	€ 6000

3.2.3 Semikwantitatief

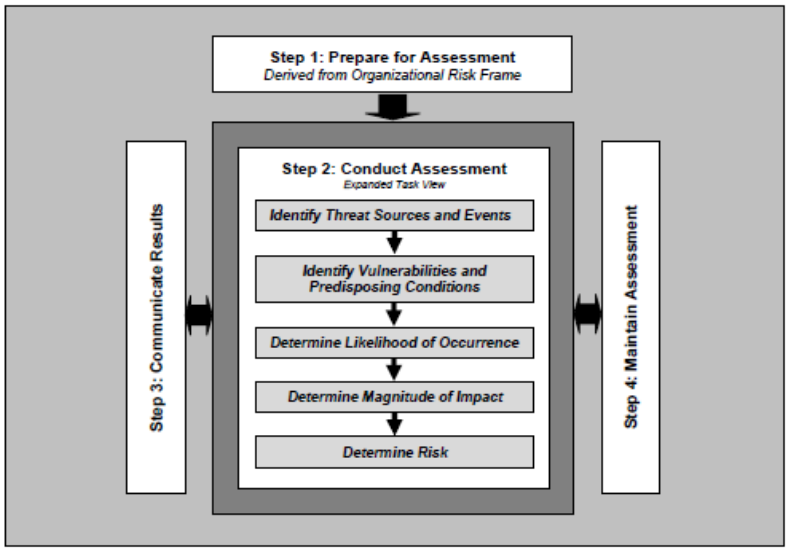
Een semikwantitatieve beoordeling biedt zowel de voordelen van de kwantitatieve als de voordelen van de kwalitatieve methode en maakt gebruik van een risicobeoordeling welke gebruik maakt van schalen (bijv. 1-7, 8-14 en 15-25) welke eenvoudig te zijn vertalen in kwalitatieve termen (bijv. een score van "20" kan worden geïnterpreteerd als "hoog"). Net als met de niet-numerieke categorieën die worden toegepast in de kwalitatieve beoordeling, dient elke schaal te worden verduidelijkt met een zinvolle omschrijving (NIST, 2012).

Likelihood	Description	Impact	Description	Risk	Description
1	Once every 5 years	1	Very low	1 - 7	Low
2	Once every 2 years	2	Low		
3	Once every year	3	Medium	8 - 14	Medium
4	2 - 5 times a year	4	High		
5	More than 5 times a year	5	Very high	15 - 25	High

Risk = likelihood x impact

3.3 Aanpak

Onderstaande aanpak is gebaseerd op de standaard van het National Institute of Standards and Technology (NIST): Guide for Conducting Risk Assessments (Special Publication 800-30):



Stap 1	**Prepare for the assessment**	**Voorbereiding van de risicoanalyse (met de afbakening/ scope en het doel van de analyse)**
Stap 2	**Conduct the assessment**	**Uitvoeren van de risicoanalyse, met:**
	Identify threat sources and events	*Bepalen welke (voor de organisatie relevante) calamiteiten zich kunnen voordoen*
	Identify vulnerabilities (and predisposing conditions)	*Bepalen welke (mogelijke) kwetsbaarheden aanwezig zijn*
	Determine likelihood of occurrence	*Bepalen van de kans dat calamiteiten zich kunnen voordoen*
	Determine magnitude of impact	*Bepalen van de impact in het geval calamiteiten zich voordoen*
	Determine risk	*Bepalen van de risicobeoordeling (berekening: kans x impact = risico)*
Stap 3	**Communicate results**	**Documenteer de aanpak en resultaten**
Stap 4	**Maintain assessment**	**Onderhouden van de risicoanalyse (up-to-date houden van de risicoanalyse documentatie)**

Bijlage 2 - Process analysis

1. Introduction

This document describes the primary business processes within Tsubakimoto Europe B.V. The primary business processes need to be mapped on order to determine which business processes are crucial regarding the continuity of the organization and which IT systems are involved in these processes.

The primary business processes are categorized by their corresponding departments. The primary business processes will be described in chapter two. The relationship between the IT systems and primary business processes is schematically represented by a table in chapter three.

2. Business processes

2.1 Sales

2.1.1 Control Debtors

When a request is made to enter or change a debtor in the system, the debtor sheet will be filled in and authorized by the Sales Manager. In case when a payment condition is present on an account, the creditworthiness of the customer is checked using a D&B report. After approval of the Sales Manager, it will be checked if a customer may already be present in the system and whether there are any open payments. The Sales Manager will fill in the debtor sheet if a debtor does not yet exist in the system (Tsubakimoto Europe B.V., 2014).

2.1.2 Margin Control & Invoicing

The Sales Manager checks the margin of all sales orders according to the information on the margin list and based on the information from the packing slip. The selling price, margin and other costs will be listed on the margin list. After authorization, the Sales Manager will archive the margin list. The Sales Manager will inform the reception that the delivery notes can be invoiced, and the original invoice is sent to the customer (Tsubakimoto Europe B.V., 2013).

2.1.3 Sales Order

An order can either be placed using fax, telephone or e-mail. It will be determined whether it's a new order, if the order already exists in the system or if an existing order needs to be changed. In case of an existing order, it will be checked whether it's still possible to modify or add information to the order. When the order is complete concerning an STP article or an assembly article, the order confirmation will be sent to the customer. MTP articles will be checked by the Sales department first, as soon as a confirmation is received from the supplier. Then, the order confirmation will be sent to the customer (Tsubakimoto Europe B.V., 2015).

2.1.4 Sales Quotation

A quotation request can either be received via fax, telephone or e-mail. A confirmation of receipt is sent to the customer if the request is accepted. It will then be determined whether the request applies to a new MTP article, or an existing STP article. When the article category is determined, the form regarding a quotation request, will be filled in. It will then be judged if it's a local quote, or that the quotation has must be sent to the supplier. In case of a local quote, the purchase price will be calculated. In case no local quote is available, the supplier will be requested to send a quotation. When the quotation of the supplier is checked on delivery time, quantity and purchase price, the article will be entered in the

system. If the quotation is prepared and the selling price has been calculated, the quotation will be sent to the customer by e-mail after authorization (Tsubakimoto Europe B.V., 2015).

2.2 Purchase

2.2.1 Creating Article Record

When a request is made to create a new article, the Purchase department will check whether the article already exists in the system. When the type of the article has been defined, it will be created in the system. STP products are created by STP-procurement, MTP products are created by MTP-procurement and assembly products are created by Sales (Tsubakimoto Europe B.V., 2015).

2.2.2 Purchase order/ confirmation

Regarding the ordering process, an STP article or an MTP article can be purchased. When an order is placed, the price, exchange rate and delivery date will be checked by the Purchase department. When the ordering process is complete, the order will be sent to the supplier. When an order confirmation is received from the supplier, the Sales department checks the price, delivery date and quantity match with the details of the order (Tsubakimoto Europe B.V., 2015).

2.3 Warehouse

2.3.1 Order collection, packing & shipment

The Warehouse Manager creates packing slips based on the orders to be sent. Orders are picked in the warehouse and will then be signed. It will then be checked whether the right goods have been collected. When the goods are packaged for shipment and signed off the packing slip, the total weight of the shipment will be checked. Upon approval, the packing slip will be placed on the shipment and the goods are ready to be shipped (Tsubakimoto Europe B.V., 2015).

2.3.2 Receipt of Goods & Warehousing

Stickers are made upon receipt of goods based in the pre-receipt number, product code and location. The received goods are then checked by the Warehouse department on any possible damage before they are stored. Then, the product code and the location where the goods are stored will be scanned. When the goods are stored at the correct location, the stock will be updated in the system (Tsubakimoto Europe B.V., 2013).

2.4 IT

2.4.1 Backup Procedure

A backup of the servers will be placed automatically on the (internal) EMC data backup server on a daily basis (in the evenings). The backup of the virtual servers will be conducted by Veeam. There is also an additional backup job scheduled, regarding the e-mail servers, which is carried out every last Saturday of the month. All files on the data server are backed up by Symantec Backup Exec. A full backup is scheduled every Friday and on weekdays (except Fridays), an incremental backup is conducted. Another full backup is scheduled on every last Sunday of the month, with a retention of 52 weeks. The backups are checked every morning and the results are stored in a backup log. The backups are then replicated (on a daily basis) to the external data center (Tsubakimoto Europe B.V., 2014).

2.4.2 Restore Procedure

The IT department decides when the restore procedure should be performed. When file restoration is required (i.e. due to the loss of files), Symantec Backup Exec will be used for recovery (from the EMC data backup server. In case of a server failure, Veeam will be used for recovery. When a restore process

is complete, it will be checked whether the restore process is completed successfully (Tsubakimoto Europe B.V., 2014).

2.5 Administration

2.5.1 Manual Creditor Payments

The administration department manually selects invoices which must be paid to creditors (suppliers). Then, the payments will be entered manually in the bank software system. The administration department will check whether the payments are correctly entered in the bank software system. When this is approved, the payments will be uploaded in the bank software system (Tsubakimoto Europe B.V., 2015).

3. IT systems and business processes

Business process	Control Debtors	Margin Control & Invoicing	Sales Order	Sales Quotation	Creating Article Record	Purchase Order/ Confirmation	Order collection, packing & shipment	Receipt of Goods & Warehousing	Backup Procedure	Restore Procedure	Manual Creditor Payments
Servers (physical)											
Barracuda Message Archiver 350			X	X							
Barracuda Spam Firewall 300			X	X							
CTXSRV06	X	X	X	X	X	X	X	X			X
DATASRV03		X	X	X		X	X	X			
DBSRV01	X	X	X	X	X	X	X	X			X
EMCDD01									X	X	
LH-SAN01	X	X	X	X	X	X	X	X	X	X	X
LH-SAN02	X	X	X	X	X	X	X	X	X	X	X
LH-SAN03	X	X	X	X	X	X	X	X	X	X	X
LH-SAN04	X	X	X	X	X	X	X	X	X	X	X
VMWSRV01	X	X	X	X	X	X	X	X	X	X	X
VMWSRV02	X	X	X	X	X	X	X	X	X	X	X
Servers (VM)											
CTXSRV07	X	X	X	X	X	X	X	X			X

DBSRV02	X	X	X	X	X	X	X	X			X
DMNSRV02		X	X	X		X	X	X			
ELOSRV01	X	X	X	X		X	X				
EXCSRV02	X	X	X	X			X				
EXCSRV03	X	X	X	X			X				
FRONTENDSRV01	X	X	X	X			X				
PORTALSRV01	X	X	X	X	X	X	X	X			X
RFSRV01							X	X			
SONICSRV01						X					
SONICSRV02						X					
VEEAMSRV01									X	X	
Switches											
HP ProCurve 4208VL	X	X	X	X	X	X	X	X	X	X	X
HP ProCurve E3500YL-24G-PoE (1)	X	X	X	X	X	X	X	X	X	X	X
HP ProCurve E3500YL-24G-PoE (2)	X	X	X	X	X	X	X	X	X	X	X
HP ProCurve 2610-12/24 PWR							X	X			
Motorola RFS6000 (Primary)							X	X			
Motorola RFS6000 (Secondary)							X	X			
Router											
Cisco Router C8536			X	X			X				
Firewall											
Juniper Firewall SSG140			X	X			X				

Bijlage 3 - IT component analysis

1. Introduction

This document provides the IT system inventory of Tsubakimoto Europe B.V. and may be consulted when a disaster occurs within the IT environment (and due to a disaster, new IT equipment needs to be purchased). This document describes the following IT equipment, along with the necessary IT system requirements: servers (both physical and virtual), switches, the router and the firewall.

The physical servers are defined in chapter two. Chapter three describes the virtual servers. In chapter four, the switches are described. Chapter five displays a brief description of the router and the firewall will be described in chapter six.

2. Servers (physical)

Barracuda Message Archiver 350			
Model:	Message Archiver 350		
Manufacturer:	Barracuda		
Serial number:			
IP address:			
Domain:			
Location:	Server room 1		
Backup location:	EMCDD01	Backup frequency:	Daily
Supplier:	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities:	• *Mail archiving*		

Barracuda Spam & Spam Firewall 300			
Model:	Spam Firewall 300		
Manufacturer:	Barracuda		
Serial number:	BAR-SF-394788		
IP address:	192.168.65.235		
Domain:	TSUBAKI.CORP		
Location:	Server room 1		
Backup location:	EMCDD01	Backup frequency:	Daily
Supplier:	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities:	• *Spam filtering*		

CTXSRV06			
Model:	ProLiant DL360p Gen8		
Manufacturer:	HP		
Serial number:			
Processor:	2 x 12-Core 2GHz Intel Xeon CPU E5-2620 0 @ 2.00GHz		
Memory:	32 GB		
Disk space:	136 GB	RAID configuration:	RAID 1
Operating System:	Microsoft Windows Server 2008 R2 Standard		
License code:			
IP address:			
Domain:			
Location:	Server room 1		
Power supply:	460W	Amount:	2
Backup location:	EMCDD01	Backup frequency:	Daily *(Veeam endpoint backup, 1 retention point)*
Supplier:	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities:	• *Application virtualization via Citrix*		

DATASRV03				
Model:	ProLiant DL360p Gen8			
Manufacturer:	HP			
Serial number:				
Processor:	12-Core 2GHz Intel Xeon CPU E5-2620 0 @ 2.00GHz			
Memory:	20 GB			
Disk space:	136 GB	RAID configuration:	RAID 1	
	3,6 TB		RAID 50	
Operating System:	Microsoft Windows Server 2012 Standard			
License code:				
IP address:				
Domain:				
Location:	Server room 1			
Power supply:	460W	Amount:	2	
Backup location:	EMCDD01	Backup frequency:	Friday:	*Full*
			Weekdays:	*Incremental*
			Monthly:	*Full*
Supplier:	Unit4			
	Stationspark 1000, 3364 DA Sliedrecht			
	T.: (0184) 44 44 44			
Functionalities:	• *Fileserver*			
	• *Limis*			
	• *Second Domain Controller*			

DBSRV01			
Model:	ProLiant DL380p Gen8		
Manufacturer:	HP		
Serial number:			
Processor:	2 x 12-Core 2GHz Intel Xeon CPU E5-2620 0 @ 2.00GHz		
Memory:	32 GB		
Disk space:	546 GB	RAID configuration:	RAID 1 + 0
Operating System:	Microsoft Windows Server 2008 R2 Standard		
License code:			
IP address:			
Domain:			
Location:	Server room 1		
Power supply:	450W	Amount:	2
Backup location:	EMCDD01	Backup frequency:	Daily *(Veeam endpoint backup, 1 retention point)*
	AW Database		Daily *(1 retention point)*
Supplier:	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities:	• *Agresso Wholesale backup*		

EMCDD01			
Model:	Data Domain DD160		
Manufacturer:	EMC		
Serial number:			
IP address:			
Domain:	TSUBAKI.CORP		
Location:	Server room 1		
Power supply:	- - -	Amount:	1
Supplier:	NedPortal		
	Londen 12, 2993 LA Barendrecht		
	T.: (088) 557 03 33		
Functionalities:	• *Backup and replication to offsite location*		

EMCDD02			
Model:	Data Domain DD160		
Manufacturer:	EMC		
Serial number:			
IP address:			
Location:	Dataplace B.V.		
	Van Coulsterweg 6, 2952 CB Alblasserdam		
	T.: (088) 328 27 52		
Power supply:	- - -	Amount:	1
Supplier:	NedPortal		
	Londen 12, 2993 LA Barendrecht		
	T.: (088) 557 03 33		
Functionalities:	• *Offsite backup*		

LH-SAN01			
Model:	StorageWorks P4300 G2		
Manufacturer:	HP		
Serial number:			
Memory:	8GB		
Disk space:	7,2 TB	RAID configuration:	RAID 5
		RAID network configuration:	RAID 10 + 1
IP address:			
Domain:			
Location:	Server room 1		
Power supply:	750W	Amount:	2
Supplier:	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities:	• *SAN Storage*		

LH-SAN02			
Model:	StorageWorks P4300 G2		
Manufacturer:	HP		
Serial number:			
Memory:	8 GB		
Disk space:	7,2 TB	RAID configuration:	RAID 5
		RAID network configuration:	RAID 10 + 1
IP address:			
Domain:			
Location:	Server room 2		
Power supply:	750W	Amount:	2
Supplier:	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities:	• *SAN Storage*		

LH-SAN03			
Model:	StoreVirtual 4330		
Manufacturer:	HP		
Serial number:			
Memory:	8 GB		
Disk space:	7,2 TB	RAID configuration:	RAID 5
		RAID network configuration:	RAID 10 + 1
IP address:			
Domain:			
Location:	Server room 1		
Power supply:	460W	Amount:	2
Supplier:	NedPortal		
	Londen 12, 2993 LA Barendrecht		
	T.: (088) 557 03 33		
Functionalities:	• *SAN Storage*		

LH-SAN04			
Model:	StoreVirtual 4330		
Manufacturer:	HP		
Serial number:			
Memory:	8 GB		
Disk space:	7,2 TB	RAID configuration:	RAID 5
		RAID network configuration:	RAID 10 + 1
IP address:			
Domain:			
Location:	Server room 2		
Power supply:	460W	Amount:	2
Supplier:	NedPortal		
	Londen 12, 2993 LA Barendrecht		
	T.: (088) 557 03 33		
Functionalities:	• *SAN Storage*		

VMWSRV01			
Model:	ProLiant DL380p Gen8		
Manufacturer:	HP		
Serial number:			
Processor:	2 x 8-Core 2GHz Intel Xeon CPU E5-2650 0 @ 2.00GHz		
Memory:	96 GB		
Disk space:	130 GB	RAID configuration:	RAID 1
Operating System:	VMware ESXi 5.1.0		
License code:			
IP address:			
Domain:			
Location:	Server room 1		
Power supply:	750W	Amount:	2
Backup location:	EMCDD01		
Supplier:	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities:	• *Part of the VMware environment*		

VMWSRV02			
Model:	ProLiant DL380p Gen8		
Manufacturer:	HP		
Serial number:			
Processor:	2 x 8-Core 2GHz Intel Xeon CPU E5-2650 0 @ 2.00GHz		
Memory:	96 GB		
Disk space:	130 GB	RAID configuration:	RAID 1
Operating System:	VMware ESXi 5.1.0		
License code:			
IP address:			
Domain:			
Location:	Server room 2		
Power supply:	750W	Amount:	2
Backup location:	EMCDD01		
Supplier:	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities:	• *Part of the VMware environment*		

3. Servers (VM)

ARSRV01			
Memory:	8 GB		
Provisioned storage:	60 GB		
Operating System:	Microsoft Windows Server 2012		
IP address:			
Domain:			
Operates on server:	VMWSRV01		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *Eagle Presence Registration*		

CRMSRV02			
Memory:	4 GB		
Provisioned storage:	50 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV01		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *Unit4 CRM*		

CTXSRV07			
Memory:	8 GB		
Provisioned storage:	80 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV01		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *Powerfuse 2012*		
	• *Citrix XenApp 6.5 Advanced Edition*		

DBSRV02			
Memory:	4 GB		
Provisioned storage:	90 GB		
Operating System:	Microsoft Windows Server 2012		
IP address:			
Domain:			
Operates on server:	VMWSRV01		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *Agresso Wholesale failover*		

DMNSRV02			
Memory:	4 GB		
Provisioned storage:	40 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV02		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *Domain Controller*		
	• *Safeword Token Database*		
	• *Domain related tasks*		
	• *Citrix License server*		
	• *Print server*		

ELOSRV01			
Memory:	8 GB		
Provisioned storage:	200 GB		
Operating System:	Microsoft Windows Server 2012		
IP address:			
Domain:			
Operates on server:	VMWSRV01		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *ELO Digital Archive*		

EXCSRV02			
Memory:	15 GB		
Provisioned storage:	200 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV01		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
	12 copies		Monthly *(last saturday of every month)*
Functionalities:	• *Microsoft Exchange 2010*		

EXCSRV03			
Memory:	15 GB		
Provisioned storage:	200 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV02		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
	12 copies		Monthly *(last saturday of every month)*
Functionalities:	• *Microsoft Exchange 2010*		

FRONTENDSRV01			
Memory:	8 GB		
Provisioned storage:	60 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV02		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
	12 copies		Monthly *(last saturday of every month)*
Functionalities:	• *Connectivity mobile devices*		

PORTALSRV01			
Memory:	4 GB		
Provisioned storage:	40 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV01		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *DMZ*		
	• *Citrix XenApp Portal*		

RFSRV01			
Memory:	8 GB		
Provisioned storage:	80 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV01		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *RF system*		
SONICSRV01			
Memory:	8 GB		
Provisioned storage:	60 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV02		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *EDI Live Environment*		

SONICSRV02			
Memory:	4 GB		
Provisioned storage:	60 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV02		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *EDI Test Environment*		
	• *TopDesk*		

TLSSRV02			
Memory:	8 GB		
Provisioned storage:	160 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV02		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *McAfee Epolicy Orchestrator 5.1*		
	• *WSUS*		
	• *Veeam One Monitor*		

VEEAMSRV01			
Memory:	4 GB		
Provisioned storage:	40 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV02		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *Veeam 8.0*		

VPNSRV01			
Memory:	8 GB		
Provisioned storage:	60 GB		
Operating System:	Microsoft Windows Server 2012		
IP address:			
Domain:			
Operates on server:	VMWSRV01		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *Routing and Remote Access*		
	• *Safeword*		

VSPHERE01			
Memory:	8 GB		
Provisioned storage:	130 GB		
IP address:			
Domain:			
Operates on server:	VMWSRV01		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily

WEBSRV03			
Memory:	8 GB		
Provisioned storage:	60 GB		
Operating System:	Microsoft Windows Server 2008 R2		
IP address:			
Domain:			
Operates on server:	VMWSRV02		
Backup location:	EMCDD01		
Backup Retention:	14 copies	Scheduled:	Daily
Functionalities:	• *DMZ*		
	• *Unit4 WebSolutions*		

4. Switches

HP ProCurve 2920-24G-PoE	
Model:	ProCurve 2920-24G-PoE
Manufacturer:	HP
Ethernet ports:	*None*
Gigabit ports:	24
VLAN:	
IP address:	
Domain:	
Location:	Server room 1
Supplier:	LanTel
	Pieter Zeemanweg 57, 3316 GZ Dordrecht
	T.: (078) 630 55 55
Functionalities:	• *Accesspoints from Aerohive WiFi are connected to this switch*

HP ProCurve Switch 4208VL	
Model:	ProCurve 4208VL
Manufacturer:	HP
Ethernet ports:	164
Gigabit ports:	20
VLAN:	
IP address:	
Domain:	
Location:	Server room 1
Supplier:	Unit4
	Stationspark 1000, 3364 DA Sliedrecht
	T.: (0184) 44 44 44
Functionalities:	• *Main switch (core switch)*

HP ProCurve Switch E3500YL-24G-PoE (LH-Switch_1)	
Model:	ProCurve Switch E3500YL-24G-PoE
Manufacturer:	HP
Ethernet ports:	*None*
Gigabit ports:	24
VLAN:	
IP address:	
Domain:	
Location:	Server room 1
Supplier:	Unit4
	Stationspark 1000, 3364 DA Sliedrecht
	T.: (0184) 44 44 44
Functionalities:	• *Part of the VMware environment*
	• *Part of Failover environment*
	• *Part of iSCSI Network*

HP ProCurve Switch E3500YL-24G-PoE (LH-Switch_2)	
Model:	ProCurve Switch E3500YL-24G-PoE
Manufacturer:	HP
Ethernet ports:	*None*
Gigabit ports:	24
VLAN:	
IP address:	
Domain:	
Location:	Server room 2
Supplier:	Unit4
	Stationspark 1000, 3364 DA Sliedrecht
	T.: (0184) 44 44 44
Functionalities:	• *Part of the VMware environment*
	• *Part of Failover environment*
	• *Part of iSCSI Network*

HP ProCurve Switch 2610-12/24 PWR	
Model:	ProCurve 2610-12/24 PWR
Manufacturer:	HP
Ethernet ports:	28
Gigabit ports:	2
VLAN:	
IP address:	
Domain:	
Location:	Server room 1
Supplier:	Actemium
	Industrielaan 18 (Postbus 169), 6950 AD Dieren
	T.: (0313) 43 01 11
Functionalities:	• *Part of the RF environment*

Motorola RFS6000 Primary	
Model:	RFS6000
Manufacturer:	Motorola
Ethernet ports:	*None*
Gigabit ports:	8
VLAN:	
IP address:	
Domain:	
Location:	Server room 1
Supplier:	Actemium
	Industrielaan 18 (Postbus 169), 6950 AD Dieren
	T.: (0313) 43 01 11
Functionalities:	• *Controller for WiFi Accesspoints RF*

Motorola RFS6000 Secondary	
Model:	RFS6000
Manufacturer:	Motorola
Ethernet ports:	*None*
Gigabit ports:	8
VLAN:	
IP address:	
Domain:	
Location:	Server room 1
Supplier:	Actemium
	Industrielaan 18 (Postbus 169), 6950 AD Dieren
	T.: (0313) 43 01 11

5. Router

Cisco C8536	
Model:	C8536
Manufacturer:	Cisco
Location:	Server room 1
Supplier:	KPN
Functionalities:	• *Internet connection*

6. Firewall

Juniper SSG140	
Model:	SSG140
Manufacturer:	Juniper
Port 0/0	
Port 0/2	
Port 0/6	
Port 0/7	
IP address:	
Domain:	
Location:	Server room 1
Supplier:	Unit4
	Stationspark 1000, 3364 DA Sliedrecht
	T.: (0184) 44 44 44
Functionalities:	• *Gateway*
	• *VPN TUK*
	• *VPN TDEG*

Bijlage 4 - Risk analysis

1. Introduction

The five most important things to do in a risk analysis are as follows; define the purpose and scope as it helps to determine the goals of the risk analysis, identify the business functions that may be at risk, establish the most likely risks that could affect the business functions, specify the risk metrics to analyze (such as the probability of the risk occurring) and finally, determine how the results will be used (Kirvan, 2015).

Once all relevant risks have been analyzed, identify strategies to deal with only the highest risks or you can address all risk categories. The strategies you define for mitigating risks are used to help design disaster recovery strategies, which are used to create disaster recovery plans (Kirvan, 2015).

This chapter defines the purpose and scope of the risk analysis. Chapter two defines the different risk methodologies to assess risk. In chapter three, the risk categories in use are described. Chapter four schematically represents possible threats in a table. In chapter five, an impact assessment (according to the quantitative methodology) is represented in a table as well. Chapter six schematically represents a table in which the relation between the IT equipment and primary business processes are defined, which are then prioritized.

1.1 Purpose

The purpose of this risk analysis is to define the relevant and possible threats which may have a negative -- physical -- impact on the IT equipment (and data) within Tsubakimoto Europe B.V. In order to be able to take corrective (and where possible, preventive) measures against threats, it is important to identify these threats, the probability and impact of these threats when they occur and finally the priorities for recovery.

1.2 Scope

The scope of this risk analysis is determined as follows:

Within the scope:

- Threats which have a physical impact on IT equipment;
- Threats which have a physical impact on data;
- Threats are classified in four risk categories (Natural & Environmental, Criminal, Personnel and Technological);
- For this risk analysis, the quantitative method will be used, where the costs are based on lost man-hours and the probability is based on an annual occurrence.

Out of scope:

- Threats which affects software, applications, organization in general (and everything in between such as the safety of personnel);
- Threats which might affect the IT equipment and data, but do not have physical consequences (impact) or where it's not able to ascertain the effects (i.e. hacking, phishing or data leakage).

2. Risk methodology

2.1 Qualitative assessment

A qualitative assessment uses words or relative values to express risk, cost and impact (Snedaker, 2014). Qualitative methods often include subjective measures like low, medium and high (Kirvan, 2010). The range of a qualitative risk assessment however, is relatively small in most cases, making the prioritization or comparison within the set of reported risks difficult. The repeatability and reproducibility of qualitative risk assessments are increased when assessed values have meaningful annotations to each level (i.e. this value is "high" because of the following reasons...) and when tables are used to combine qualitative values (NIST, 2012).

#	Threat area	Potential threat	Probability	Impact
Criminal	Malware/ Virus attacks	*Malware or viruses are capable of data deletion, destruction or manipulation.*	Likely	Very high
	Break-ins	*Destruction or theft of IT equipment (as a consequence of a break-in).*	Rare	High
	Theft	*Theft of (confidential) data.*	Unlikely	Very High
		Theft of IT equipment.	Rare	High
	Vandalism	*Damaging/ destruction of IT equipment.*	Unlikely	High
		Damaging/ destruction of data.	Unlikely	Very High

2.2 Quantitative assessment

A quantitative assessment can be defined as observations that involve measurements and numbers. They are specific and measurable (Snedaker, 2014). The quantitative method assigns numerical values to the risk, which usually requires access to reliable statistics to project the future likelihood of risk (Kirvan, 2010). The accuracy of quantification is lessened when the subjective determinations are buried within the quantitative assessments, or when an amount of uncertainty surrounds the determination of values. However, when performed accurately, some benefits of the quantitative assessments include the exactness, repeatability and reproducibility of the assessment results (NIST, 2012).

#	Threat area	Potential threat	Annual incidents	Cost per incident	Total cost
Criminal	Malware/ Virus attacks	*Malware or viruses are capable of data deletion, destruction or manipulation.*	4	€ 2000	€ 8.000
	Break-ins	*Destruction or theft of IT equipment (as a consequence of a break-in).*	1	€ 10.000	€ 10.000
	Theft	*Theft of (confidential) data.*	2	€ 1000	€ 2000
		Theft of IT equipment.	1	€ 20.000	€ 20.000
	Vandalism	*Damaging/ destruction of IT equipment.*	1	€ 5000	€ 5000
		Damaging/ destruction of data.	2	€ 5000	€ 10.000

Total cost (Risk) = (probability) annual incidents x (impact) cost per incident

2.3 Semi-Quantitative assessment

This type of assessment can provide the benefits of quantitative and qualitative assessments and employs a set of procedures or rules for assessing risk that uses bins, scales or representative numbers. The bins (i.e. 1-7, 8-14 and 15-25) or scales (1-10) translate easily into qualitative terms that support risk communications for decision makers (i.e. a score of 20 can be interpreted as high), while also allowing relative comparisons between values in different bins or even within the same bin (i.e. the difference between risks scored 8 and 9 is relatively insignificant, while the difference between risks scored 3 and 8 is relatively significant). As with the non-numeric categories or levels used in a qualitative approach, each bin or scale of values needs to be clarified by meaningful examples (NIST, 2012).

Risk magnitude	
1 - 7	Low
8 - 14	Medium
15 - 25	High

#	Threat area	Potential threat	Probability	Impact	Risk	Magnitude
Criminal	Malware/ Virus attacks	• *Malware or viruses are capable of data deletion, destruction or manipulation.*	4	4	16	High
	Break-ins	• *Destruction or theft of IT equipment (as a consequence of a break-in).*	1	4	4	Low
	Theft	• *Theft of (confidential) data;*	2	3	6	Low
		• *Theft of IT equipment.*	2	4	8	Medium
	Vandalism	• *Damaging/ destruction of IT equipment;*	2	4	8	Medium
		• *Damaging/ destruction of data.*	2	3	6	Low

Risk = probability x impact

3. Risk categories

3.1 Natural & Environmental

Natural or environmental threats may occur everywhere, but there are some boundaries that determine whether it's more likely to experience a specific natural threat like fires, earthquakes, floods or tornadoes (Snedaker, 2014). In this case, earthquakes or tornadoes won't be occurring here, so these kind of threats will be left out of the scope. However, natural threats by means of fire or storms may occur, so these threats might be relevant. Environmental threats, such as a power outage or leakage, may be caused by natural threats or humans, and may have an effect in a specific area.

3.2 Criminal

There can be many threats regarding criminality. A great example in this case would be cyber criminality (hackers entering your IT network, stealing confidential data or might even have access to your passwords). Even though cyber criminality is really important issue to focus on in IT, it won't be present in this scope since the focus here lies with the assessment of threats which may physically affect IT equipment and data. Criminal threats which may physically affect data, are malware/ viruses (capable of deleting, altering or destroying data). Other examples of criminal threats which might have a physical affect on IT equipment or data; are theft of IT equipment and vandalism (i.e. destruction of IT equipment or data).

3.3 Personnel

Some of the biggest threats might arise from the inside; employees can either form an intentional or accidental threat to your IT equipment and data. Examples of intentional threats could be damaging IT equipment on purpose, or stealing confidential business data. Examples of accidental threats could be the accidental removal of data or accidental destruction of IT equipment.

3.4 Technological

Technological threats are those threats which arise in technology and might form a danger to IT equipment or (confidential) data. These threats may consist of hardware issues (i.e. incorrectly configured equipment might cause hardware failure) or even vendor failure might cause issues to your hardware if, for example, a vendor owns some of your equipment at a remote location.

4. Threat assessment

Possible threats which may occur within -- or may have consequences for -- the IT environment and data are listed below. The 'Threat Area' column represents the identified threats. The 'Potential threat' column represents a description of the identified threats. The 'Current bottlenecks' column represents the current weaknesses/ gaps within Tsubakimoto which might be exploited by threats.

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 of 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 (i.e. accidental deletion of data).*	• Configuration mistakes might give personnel privileged access.
	Technological	
Hardware issues/ failure	*Loss of data.*	• A backup job might fail, which might cause 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 offsite location.*	• There is currently no replacement IT equipment available (regarding a backup server).

5. Impact assessment

The probability of occurrence, impact and risk factor are represented in the table below. The probability is based on an annual occurrence, the impact is based on costs of lost man-hours and hardware costs. The risk factor is calculated by the following formula: Risk = Probability x Impact.

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 offsite location.*	0,0001	€ 6.000,00	€ 0,60

6. Prioritizing risk

Regarding weighing priorities, a priority scale of 10 - 150 will be used (the 'Priority Value'); where 150 has the lowest priority and 10 the highest priority. The 'Priorty Score' column indicates which IT system(s) should be restored as soon as possible after a disruptive event took place. The 'Priorty Score' can be calculated by adding the numbers ('Priority Value') associated with the amount of Business processes wherein a certain IT system is involved. The higher the 'Priority Score', the higher the priority (maximum score: 361).

Priority Value	***40***	***13***	***70***	***20***	***33***	***60***	***16***	***50***	***13***	***10***	***36***	#
Business process	Control Debtors	Margin Control & Invoicing	Sales Order	Sales Quotation	Creating Article Record	Purchase Order/ Confirmation	Order collection, packing & shipment	Receipt of Goods & Warehousing	Backup Procedure	Restore Procedure	Manual Creditor Payments	***Priority Score***
Servers (physical)												
Barracuda Message Archiver 350				X								***20***
Barracuda Spam Firewall 300			X	X								***90***

CTXSRV06	X	X	X	X	X	X	X	X			X	***338***
DATASRV03		X	X	X		X	X	X				***229***
DBSRV01	X	X	X	X	X	X	X	X			X	***338***
EMCDD01									X	X		***23***
LH-SAN01	X	X	X	X	X	X	X	X	X	X	X	***361***
LH-SAN02	X	X	X	X	X	X	X	X	X	X	X	***361***
LH-SAN03	X	X	X	X	X	X	X	X	X	X	X	***361***
LH-SAN04	X	X	X	X	X	X	X	X	X	X	X	***361***
VMWSRV01	X	X	X	X	X	X	X	X	X	X	X	***361***
VMWSRV02	X	X	X	X	X	X	X	X	X	X	X	***361***
Servers (VM)												
CTXSRV07	X	X	X	X	X	X	X	X			X	***338***
DBSRV02	X	X	X	X	X	X	X	X			X	***338***
DMNSRV02		X	X	X		X	X	X				***229***
ELOSRV01	X	X	X	X		X	X					***219***
EXCSRV02	X	X	X	X			X					***159***
EXCSRV03	X	X	X	X			X					***159***
FRONTENDSRV01	X	X	X	X			X					***159***
PORTALSRV01	X	X	X	X	X	X	X	X			X	***338***
RFSRV01							X	X				***66***
SONICSRV01						X						***60***
SONICSRV02						X						***60***
VEEAMSRV01									X	X		***23***
Switches												
HP ProCurve 4208VL	X	X	X	X	X	X	X	X	X	X	X	***361***
HP ProCurve E3500YL-24G-PoE (1)	X	X	X	X	X	X	X	X	X	X	X	***361***
HP ProCurve E3500YL-24G-PoE (2)	X	X	X	X	X	X	X	X	X	X	X	***361***
HP ProCurve 2610-12/24 PWR							X	X				***66***
Motorola RFS6000 (Primary)							X	X				***66***
Motorola RFS6000 (Secondary)							X	X				***66***
Router												
Cisco Router C8536			X	X			X					***106***
Firewall												
Juniper Firewall SSG140			X	X			X					***106***

Bijlage 5 - Disaster Recovery plan

Contact information

Key personnel

Name	Title	Work phone	Mobile phone	Email address

Key suppliers

Name	Contact details	
Actemium	Street	*Industrielaan 18, Postbus 169*
	Postal code	*6950 AD*
	City	*Dieren*
	Phone	*0313 - 43 01 11*
Dataplace B.V.	Street	*Van Coulsterweg 6*
	Postal code	*2952 CB*
	City	*Alblasserdam*
	Phone	*088 - 328 27 52*
LanTel	Street	*Pieter Zeemanweg 57*
	Postal Code	*3316 GZ*
	City	*Dordrecht*
	Phone	*078 - 630 55 55*
NedPortal	Street	*Londen 12*
	Postal code	*2993 LA*
	City	*Barendrecht*
	Phone	*088 - 557 03 33*
Unit4	Street	*Stationspark 1000*
	Postal code	*3364 DA*
	City	*Sliedrecht*
	Phone	*0184 - 44 44 44*

1. Organization

1.1 About

Tsubakimoto aims to be a leading company in the global markets, and will provide the best value to customers around the world by capitalizing technical strengths in power transmission products and materials handling systems.

Tsubakimoto delivers product excellence by means of fair valued technical advantages and high brand recognition, partnership with reliable delivery and people, enhanced production efficiency and solution for customers, and profitability by proven and consistent quality and service at work.

By managing the IT environment in the right way, business processes can be optimized, leading to improved business aspects such as customer satisfaction, productivity, profitability and competitiveness.

1.2 Critical business processes

Department	Business process
Sales	Control Debtors
	Margin Control & Invoicing
	Sales Order
	Sales Quotation
Purchase	Creating Article Record
	Purchase Order/ Confirmation
Warehouse	Order Collection, Packing & Shipment
	Receipt of Goods & Warehousing
IT	Backup Procedure
	Restore Procedure
Administration	Manual Creditor Payments

2. Plan overview

2.1 Purpose and scope

The purpose of this plan is to provide guidelines which need to be followed in order to adequately restore IT equipment and components -- which support the critical business processes -- that are interrupted due to a disaster. This plan also describes the roles and responsibilities of key personnel who will be responsible for making certain decisions during and after a disaster.

2.1.1 Assumptions

- This plan should cover all essential IT equipment and components in conjunction with the defined critical business processes;
- All (key) personnel are aware of their responsibilities and understands how the plan is to be executed, and are available when needed in case a disaster occurs;
- This plan should be periodically tested to ensure that it can be implemented effectively in case a disaster occurs;
- This plan, along with other relevant and necessary documents, will be stored in a safe location and has to be available when needed;

- This plan is to be maintained when changes occur in the business environment. The plan should be approved by management each time a new definitive revision has been made.

2.1.2 Objectives

- This plan serves as a guide in case disasters -- which might physically affect IT equipment, components and data -- occur within Tsubakimoto Europe B.V.;
- This plan contains procedures necessary to recover from a disaster and to be less vulnerable to the risk of disasters;
- This plan identifies key personnel and their responsibilities -- which need to be carried out in case a disaster occurs -- and who should be contacted in the event of a disaster;
- This plan identifies what corrective (and, where possible, preventive) measures should be taken in order to intervene in the event of a disaster.

2.2 Plan documentation storage

Each team leader of the Management Team, Damage Assessment Team and the IT Recovery Team should receive a printed copy and a digital copy (i.e. a copy on CD) of this Disaster Recovery plan. All copies of this plan need to be stored in secure locations within Tsubakimoto Europe B.V. and at another external location.

When a new version of the plan is available, older copies of the plan (both printed and digital copies) must be destroyed in a secure manner. The new version of the plan should then be distributed to the designated individuals.

2.3 Plan maintenance

It is necessary to review the Disaster Recovery plan regularly (i.e. every three months), to determine if the plan is still up-to-date. Possible implementation of new services, employees, vendors or IT equipment and components within Tsubakimoto Europe B.V. need to be added to the plan immediately. Each new version of the plan should be presented to the Management, and needs to be signed after approval.

2.4 Plan testing

It is essential to test the Disaster Recovery plan annually, in order to assess the degree of preparedness in case a disaster occurs within Tsubakimoto Europe B.V. In addition, the key personnel who have certain roles and responsibilities defined in this plan, should be trained annually to become aware of their roles and responsibilities in order to carry out their individual responsibilities adequately.

Testing this Disaster Recovery plan includes the following actions:

- The IT recovery procedures for all critical IT equipment and components that support the primary business functions;
- Training key personnel so that they are made aware of their roles and responsibilities defined in this Disaster Recovery plan.

3. Plan invocation

3.1 Plan triggering events

Key trigger issues at the organization that would lead to activation of the DRP are:

- Loss of IT equipment/ components and damaged IT equipment/ components;
- Loss of data, destruction of data and damaged data;
- Loss of outsourced services.

3.2 Teams and responsibilities

3.2.1 Management Team

The Management Team is responsible for making any business related decisions, which will have an impact on Tsubakimoto Europe B.V. as a company. The management team needs to ensure that the actions and decisions which need to be made by other Disaster Recovery teams, abide by the Disaster Recovery plan.

Name	Title	Work phone	Mobile phone	Email address

Roles & responsibilities

- Ensuring that all decisions made are according to the actions specified in this plan, and according to the rules, values and policies set by Tsubakimoto Europe B.V.;
- Reviewing and approving hardware investments and upgrades;
- Reviewing and approving new revisions of the plan in case changes are made;
- Ensuring there is sufficient credit available in order to deal with unexpected expenses (such as repair costs) caused by a disaster.

3.2.2 Damage Assessment Team

The Damage Assessment Team determines wether the Disaster Recovery plan should be invoked, and is responsible to assess all the issues which are related to the IT equipment and the housing location(s) that contains the IT equipment (i.e. the server rooms). The team is also responsible for assessing damage done to the IT equipment and data, and overseeing the repairs to the IT equipment and housing location(s) in the event of a disaster.

Name	Title	Work phone	Mobile phone	Email address

Roles & responsibilities

- Invocate the Disaster Recovery plan after a disaster has been reported (which meets the 'Plan triggering events' requirements specified in this plan);
- Assess which IT systems, components and processes have been affected by a disaster;
- Assess any physical damage done the IT equipment, components and data;
- Hiring temporary staff needed to recover and continue business functionality faster;

- Contact suppliers or insurance companies in case IT equipment or components need to be replaced or repaired;
- Identify and document the state of the disaster and any expected repair/ replacement costs during the damage assessment process, and report this to the Management Team.

3.2.3 IT Recovery Team

The IT Recovery Team is responsible for ensuring the functionality of IT equipment and components prior to, during and after a disaster. The IT Recovery Team is also responsible for assessing damage done to IT systems, components and data in the event of a disaster. In order to determine the nature and extent of the damage, the IT Recovery Team works closely with the Damage Assessment Team. The IT Recovery Team is also responsible to invoke the recovery and restore tasks once the Disaster Recovery plan has been activated.

Concerning the recovery of the IT systems and components (as defined in the recovery procedures in this plan), a switch, a VMware server and a SAN storage system should be available in all cases, so that these systems can communicate with each other in order to restore the IT systems and components with the appropriate backup.

Name	Title	Work phone	Home phone	Email address

Roles & responsibilities

- Assess which IT equipment and components are not able to function in the event of a disaster;
- Take measures to prevent further damage done to IT equipment, components and data;
- Communicate the occurrence and impact of a disaster to employees and if necessary, suppliers (either by phone or by email);
- Install and implement any tools or hardware needed to recover from a disaster;
- Keep the IT equipment and components up-to-date with system patches, application patches and data copies;
- Ensuring sufficient replacement peripherals, servers and components are available;
- Ensuring the Backup procedure and Restore procedure proceed appropriately;
- Ensuring that the DRP is maintained and updated regularly;
- Ensuring that the DRP is tested and reviewed regularly;
- Communicate the status of recovery to the Management Team periodically (once every hour);
- Contact the Management Team, Functional Area team and employees respectively when the affected IT systems, components and data (and thus, business functionality) have been restored;
- After all operations returned to function as usual, document[2] all steps undertaken in the recovery process and report this to the Management Team.

[2] *To document the steps undertaken in the recovery process, use the "Event Log" form provided in appendix H.*

3.2.4 Functional Area Team

The Functional Area Team consists of managers from each department involved in the critical business processes. The Functional Area Team is responsible for ensuring that the communication with employees of their corresponding department, suppliers and customers during a disaster is adequate.

Name	Title	Functional Area	Work phone	Mobile phone	Email address

Roles & responsibilities

- Ensuring that employees can resume their work within the department as much as possible;
- Take care of communication with customers during a disaster (i.e. notifying customers when a disaster has occurred and when business functionality returned to normal);
- Take care of communication with suppliers during a disaster (i.e. tracking shipments, arrange deliveries).

3.3 Communication

When a disaster has occurred, it needs to be reported to the Damage Assessment Team. The Damage Assessment Team will assess the damage in order to determine the impact of the disaster and if the Disaster Recovery plan should be invoked. The Damage Assessment Team will then report their findings (and if applicable, expected repair or replacement costs) and status to the Management Team. The Damage Assessment Team will also communicate their findings with the Functional Area Team, so that they can notify the employees, suppliers and customers of the event. The IT Recovery Team will implement the recovery procedures necessary in order to recover from a disaster. During the recovery process, the IT Recovery Team will regularly communicate (i.e. once every hour) with the Management Team and Functional Area Team about the progress.

4. Risk analysis

4.1 Threat assessment

Possible threats which may occur within -- or may have consequences for -- the IT environment and data are represented in the table below. The 'Threat Area' column represents the identified threats. The 'Potential threat' column represents a description of the identified threats. The 'Bottlenecks' column represents the current weaknesses/ gaps which might be exploited by threats.

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 of 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 (i.e. accidental deletion of data).*	• Configuration mistakes might give personnel privileged access.

	Technological	
Hardware issues/ failure	*Loss of data.*	• A backup job might fail, which might cause 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 offsite location.*	• There is currently no replacement IT equipment available (regarding a backup server).

4.2 Impact assessment

The probability of occurrence, impact and risk factor are represented in the table below. The probability is based on an annual occurrence, the impact is based on costs of lost man-hours and hardware costs. The risk factor is calculated by the following formula: *Risk = Probability x Impact*.

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 offsite location.*	0,0001	€ 6.000,00	€ 0,60

5. IT environment

5.1 Key IT equipment

An inventory of the IT systems and components[3] (servers, switches, the router and the firewall) is represented in the table below.

Type	Name
Servers (physical)	Barracuda Message Archiver 350
	Barracuda Spam Firewall 300
	CTXSRV06
	DATASRV03
	DBSRV01
	EMCDD01
	LH-SAN01
	LH-SAN02
	LH-SAN03
	LH-SAN04
	VMWSRV01
	VMWSRV02
Servers (VM)	ARSRV01
	CRMSRV02
	CTXSRV07
	DBSRV02
	DMNSRV02
	ELOSRV01
	EXCSRV02
	EXCSRV03
	FRONTENDSRV01
	PORTALSRV01
	RFSRV01
	SONICSRV01
	SONICSRV02

[3] *A detailed description of the IT systems and components is provided in the "IT system inventory" in Appendix B.*

	TLSSRV02
	VEEAMSRV01
	VPNSRV01
	VSPHERE01
	WEBSRV03
Switches	HP ProCurve 2920-24G-PoE
	HP ProCurve 4208VL
	HP ProCurve E3500YL-24G-PoE (1)
	HP ProCurve E3500YL-24G-PoE (2)
	HP ProCurve 2610-12/24 PWR
	Motorola RFS6000 (Primary)
	Motorola RFS6000 (Secondary)
Router	Cisco Router C8536
Firewall	Juniper Firewall SSG140

5.2 Backup policy

The backup schedules are represented in the table below. Server-images and virtual machines are backed up by Veeam Endpoint Backup. Files on the data server are backed up by Symantec Backup Exec.

Name	Backup location	Backup retention	Scheduled
Servers (physical)			
Barracuda Message Archiver 350	EMCDD01	- - -	Daily
Barracuda Spam Firewall 300	EMCDD01	- - -	Daily
CTXSRV06	EMCDD01	1 copy	Daily
DATASRV03	EMCDD01	1 copy	Daily
DBSRV01	EMCDD01	1 copy	Daily
	AW Database	1 copy	Daily
Servers (VM)			
ARSRV01	EMCDD01	14 copies	Daily
CRMSRV02	EMCDD01	14 copies	Daily
CTXSRV07	EMCDD01	14 copies	Daily
DBSRV02	EMCDD01	14 copies	Daily
DMNSRV02	EMCDD01	14 copies	Daily
ELOSRV01	EMCDD01	14 copies	Daily
EXCSRV02	EMCDD01	14 copies	Daily
		12 copies	Monthly
EXCSRV03	EMCDD01	14 copies	Daily
		12 copies	Monthly
FRONTENDSRV01	EMCDD01	14 copies	Daily
		12 copies	Monthly
PORTALSRV01	EMCDD01	14 copies	Daily
RFSRV01	EMCDD01	14 copies	Daily
SONICSRV01	EMCDD01	14 copies	Daily
SONICSRV02	EMCDD01	14 copies	Daily
TLSSRV02	EMCDD01	14 copies	Daily
VEEAMSRV01	EMCDD01	14 copies	Daily

VPNSRV01	EMCDD01	14 copies	Daily
VSPHERE01	EMCDD01	14 copies	Daily
WEBSRV03	EMCDD01	14 copies	Daily

Name	Backup location	Backup retention	Scheduled	
DATASRV03	EMCDD01	1 week	Weekdays	*Incremental backup*
		5 weeks	Friday	*Full backup*
		52 weeks	Sunday	*Full backup*

6. Recovery measures

6.1 Priorities for recovery

The table below represents the priorities for recovery[4], in order to determine which IT system(s) should be restored as soon as possible after a disruptive event took place.

Regarding weighing priorities, a priority scale of 10 - 150 will be used as the 'Priority Value', where 150 has the lowest priority and 10 the highest priority. The 'Priorty Score' can be calculated by adding the numbers ('Priority Value') associated with the amount of Business processes wherein a certain IT system is involved. The higher the 'Priority Score', the higher the priority (maximum score: 361).

Priority Value	***40***	***33***	***20***	***70***	***60***	***50***	***16***	***13***	***36***	***13***	***10***	**#**
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	***Priority Score***
Servers (physical)												
Barracuda Message Archiver 350			X									***20***
Barracuda Spam Firewall 300			X	X								***90***
CTXSRV06	X	X	X	X	X	X	X	X	X			***338***
DATASRV03			X	X	X	X	X	X				***229***

[4] *To restore the IT systems and components in a specific order, see the "IT recovery startup sequence" procedure provided in Appendix G.*

DBSRV01	X	X	X	X	X	X	X	X	X			***338***
EMCDD01										X	X	***23***
LH-SAN01			X	X		X	X	X	X	X	X	***228***
LH-SAN02			X	X		X	X	X	X	X	X	***228***
LH-SAN03			X	X		X	X	X	X	X	X	***228***
LH-SAN04			X	X		X	X	X	X	X	X	***228***
VMWSRV01	X	X	X	X	X	X	X	X	X	X	X	***361***
VMWSRV02	X	X	X	X	X	X	X	X	X	X	X	***361***
Servers (VM)												
CTXSRV07	X	X	X	X	X	X	X	X	X			***338***
DBSRV02	X	X	X	X	X	X	X	X	X			***338***
DMNSRV02			X	X	X	X	X	X				***229***
ELOSRV01	X		X	X	X		X	X				***219***
EXCSRV02	X		X	X			X	X				***159***
EXCSRV03	X		X	X			X	X				***159***
FRONTENDSRV01	X		X	X			X	X				***159***
PORTALSRV01	X	X	X	X	X	X	X	X	X			***338***
RFSRV01						X	X					***66***
SONICSRV01					X							***60***
SONICSRV02					X							***60***
VEEAMSRV01										X	X	***23***
Switches												
HP ProCurve 4208VL	X	X	X	X	X	X	X	X	X	X	X	***361***
HP ProCurve E3500YL-24G-PoE (1)	X	X	X	X	X	X	X	X	X	X	X	***361***
HP ProCurve E3500YL-24G-PoE (2)	X	X	X	X	X	X	X	X	X	X	X	***361***
HP ProCurve 2610-12/24 PWR						X	X					***66***
Motorola RFS6000 (Primary)						X	X					***66***
Motorola RFS6000 (Secondary)						X	X					***66***
Router												
Cisco Router C8536			X	X			X					***106***
Firewall												
Juniper Firewall SSG140			X	X			X					***106***

The procedures for restoring IT systems and components[5], data[6], and mailbox items[7] are enclosed in separate appendices.

6.2 Corrective and preventive measures

The corrective (and where possible, preventive) measures have been defined for each threat which have been identified during the risk analysis. The existing controls to reduce certain risks, which already have been implemented within Tsubakimoto Europe B.V., are also described in this chapter.

6.2.1 Fire

The existing controls which have been implemented to reduce the risk of a fire, are as follows:

- A fire alarm has been implemented throughout the facility;
- A fire exercise is carried out twice a year (to create personnel awareness of the evacuation process);
- Annual checkups regarding fire safety within the facility are carried out by the fire department;
- The facility has fire-proof walls.

IT equipment and components should regularly be checked to ensure the equipment is working properly. Possible defects in hardware or components may cause a fire (such as an overheating power supply), so it is important to maintain and check the IT equipment regularly to avoid (and repair) possible defects in time. Implementing a smoke detection system may reduce the impact of a fire since smoke detection systems generate an alarm if smoke is detected, so that significant damage can be avoided. Maintaining the fire-fighting equipment (such as fire extinguishers) also contributes to reducing the impact of a fire, since it is very important to have these kind of tools in case of a fire.

The following **corrective** measures can be taken to reduce the risk of a fire:

- Regularly check IT equipment and components;
- Implement a smoke detection system;
- Maintain fire-fighting equipment.

6.2.2 Water damage

Roofs and pipes should be checked regularly for possible leaks or bursts, which might cause water damage. The roof should be cleared from snow and ice during the winter to prevent leakage (which may also cause water damage).

The following **corrective** measures can be taken to reduce the risk of water damage:

- Regularly check roofs and pipes for throughout the facility.

The following **preventive** measures can be taken to avoid water damage:

- Clear the roof from snow and ice during winter.

6.2.3 Power outage

The existing controls which have been implemented to reduce the risk of a power outage, are as follows:

- An Uninterruptible Power Supply (UPS) is available within the facility;

[5] *A detailed description of the IT systems restore process is provided in Appendix C ("IT system restore procedures").*
[6] *A detailed description of the File restore process is provided in Appendix D ("File restore procedure").*
[7] *A detailed description of the Mailbox items restore process is provided in Appendix E ("Microsoft Exchange 2010 restore procedure").*

- Lightning rods are implemented on the roof of the facility.

Cables and sockets within the facility should be maintained and checked regularly (i.e. cable insulation damage), to reduce the possibility of a power outage. IT equipment is susceptible to dust and should therefore be maintained and cleaned regularly to prevent a power outage due to overheating of these systems.

The following **corrective** measures can be taken to reduce the risk of a power outage:
- Regularly maintain and check cables, sockets and other electrical equipment/ components for possible damage.

6.2.4 Malware/ Virus attacks

The existing controls which have been implemented to reduce the risk of malware/ virus attacks, are as follows:
- McAfee anti-virus has been implemented which scans the IT systems regularly to reduce the risk of being vulnerable to malware/ virus attacks;
- A (physical) Firewall has been implemented in the IT environment;
- Operating systems and McAfee anti-virus software are updated regularly;
- When a virus attack took place, the affected driver (location) will be isolated in order to scan and repair the system adequately (the “Anti-virus breakout control” module in McAfee).

To reduce the risk of some malware/ viruses affecting the IT systems (even though a sufficient anti-virus such as McAfee has been implemented), an additional anti-virus or anti-malware software program could be installed on the IT systems to scan for potential malware/ virus attacks (since some anti-virus software programs can detect particular types of malware/ viruses). Another way to reduce the risk of malware/ virus attacks, is to create awareness amongst personnel about possible ways of malware/ viruses entering an IT system (to avoid data loss or data modification due to a malware/ virus attack, regularly backup data).

The following **corrective** measures can be taken to reduce the risk of a malware/ virus attack:
- Install additional anti-virus software products which may detect a broader variety of malware/ viruses than the currently installed McAfee anti-virus program;
- Create awareness amongst personnel about malware/ virus attacks and spreading.

6.2.5 Burglary

The existing controls which have been implemented to reduce the risk of burglary (vandalism and theft), are as follows:
- ‘Motion detection’ lighting has been implemented outside of the facility;
- An alarm and camera system have been implemented throughout the facility;
- Both server rooms are locked.

Even though both server rooms are locked, it may also be necessary to lock the server and component racks when the building is empty (preventing a third party accessing the equipment in case someone broke into one of the server rooms). Unattended access to the server rooms should be avoided. Important items, equipment and other components should be stored in a safe or other environment to prevent equipment loss due to theft or vandalism. Purchase replacement IT equipment and regularly backup data to prevent equipment loss and data loss.

The following **corrective** measures can be taken to reduce the risk of theft and vandalism:

- Make sure to lock the server and component racks.

The following **preventive** measures can be taken to avoid theft and burglary:

- Keep important items, equipment and components in a locked safe;
- Don't allow access in the server rooms unattended;
- Regularly backup data (once every hour) to prevent data loss.
- Purchase replacement IT equipment (such as servers and switches).

6.2.6 Accidental actions

There is a possibility that personnel might alter or delete data accidentally, which might cause loss (or change) of data. It is important to backup data regularly to prevent data loss in such cases. Currently, all (confidential) data is backed up on a daily basis (once per day). To ensure no data will be lost in such situations, data should be backed up regularly (i.e. once every hour).

The following **preventive** measures can be taken to avoid data loss:

- Regularly backup data (once every hour).

6.2.7 Hardware issues/ failure

The existing controls which have been implemented to reduce the possibility of data loss, loss of IT equipment and loss of network connectivity, are as follows:

- All physical servers have redundant power supplies;
- Data is backed up on a daily and monthly basis;
- The server rooms are properly ventilated which prevents the IT equipment to overheat;
- The secondary (redundant) backup server is located within an offsite facility.

To reduce the possibility of hardware failure and loss of network connectivity, old hardware in use should be replaced. For example; even though the core switch, firewall and router currently in use still function it should be considered to replace these hardware components since the hardware might be outdated. Another action that could be taken to reduce the possibility of hardware failure, is to maintain hardware and components regularly. Servers can also be monitored for signs of possible errors or other future problems, in order to repair them quickly and reduce the risk of equipment failure. Purchase replacement IT equipment and regularly backup data to prevent equipment loss and data loss.

The following **corrective** measures can be taken to reduce the possibility of hardware issues/ failure:

- Replace old hardware in use;
- Maintain (and check) the hardware regularly for possible defects;
- Monitor servers for signs of possible errors or other future problems.

The following **preventive** measures can be taken to avoid data loss and hardware issues/ failure:

- Regularly backup data (once every hour).
- Purchase replacement components such as hard disks and power supplies of replacement of compartments is necessary;
- Purchase replacement IT equipment (such as servers and switches).

6.2.8 Vendor failure

Even though the secondary backup server of Tsubakimoto Europe B.V. is located within an offsite facility, there is still a possibility that the secondary backup server might be lost (i.e. due to a fire). A preventive measure that can be taken to avoid equipment loss in a way, is to purchase replacement equipment. This way the secondary backup server can be replaced immediately in case the equipment fails (or might be lost) due to a disruption at the vendor's facility.

The following **preventive** measures can be taken to avoid equipment loss:

- Purchase replacement IT equipment (in this case, a backup server).

Appendix A - IT network drawing

Appendix B - IT system inventory

Servers (physical)

Barracuda Message Archiver 350			
Model	Message Archiver 350		
Manufacturer	Barracuda		
Serial number			
IP address			
Domain			
Location	Server room 1		
Backup location	EMCDD01	Backup frequency	Daily
Supplier	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities	• *Mail archiving*		

Barracuda Spam & Spam Firewall 300			
Model	Spam Firewall 300		
Manufacturer	Barracuda		
Serial number			
IP address			
Domain			
Location	Server room 1		
Backup location	EMCDD01	Backup frequency	Daily
Supplier	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities	• *Spam filtering*		

CTXSRV06			
Model	ProLiant DL360p Gen8		
Manufacturer	HP		
Serial number			
Processor	2 x 12-Core 2GHz Intel Xeon CPU E5-2620 0 @ 2.00GHz		
Memory	32 GB		
Disk space	136 GB	RAID configuration	RAID 1
Operating System	Microsoft Windows Server 2008 R2 Standard		
License code			
IP address			
Domain			
Location	Server room 1		
Power supply	460W	Amount	2
Backup location	EMCDD01	Backup frequency	Daily *(Veeam endpoint backup, 1 retention point)*
Supplier	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities	• *Application virtualization via Citrix*		

DATASRV03				
Model	ProLiant DL360p Gen8			
Manufacturer	HP			
Serial number				
Processor	12-Core 2GHz Intel Xeon CPU E5-2620 0 @ 2.00GHz			
Memory	20 GB			
Disk space	136 GB	RAID configuration	RAID 1	
	3,6 TB		RAID 50	
Operating System	Microsoft Windows Server 2012 Standard			
License code				
IP address				
Domain				
Location	Server room 1			
Power supply	460W	Amount	2	
Backup location	EMCDD01	Backup frequency	Friday:	*Full*
			Weekdays:	*Incremental*
			Monthly:	*Full*
Supplier	Unit4			
	Stationspark 1000, 3364 DA Sliedrecht			
	T.: (0184) 44 44 44			
Functionalities	• *Fileserver*			
	• *Limis*			
	• *Second Domain Controller*			

DBSRV01			
Model	ProLiant DL380p Gen8		
Manufacturer	HP		
Serial number			
Processor	2 x 12-Core 2GHz Intel Xeon CPU E5-2620 0 @ 2.00GHz		
Memory	32 GB		
Disk space	546 GB	RAID configuration	RAID 1 + 0
Operating System	Microsoft Windows Server 2008 R2 Standard		
License code			
IP address			
Domain			
Location	Server room 1		
Power supply	450W	Amount	2
Backup location	EMCDD01	Backup frequency	Daily *(Veeam endpoint backup, 1 retention point)*
	AW Database		Daily *(1 retention point)*
Supplier	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities	• *Agresso Wholesale backup*		

EMCDD01			
Model	Data Domain DD160		
Manufacturer	EMC		
Serial number			
IP address			
Domain			
Location	Server room 1		
Power supply	- - -	Amount	1
Supplier	NedPortal		
	Londen 12, 2993 LA Barendrecht		
	T.: (088) 557 03 33		
Functionalities	• *Backup and replication to offsite location*		

EMCDD02			
Model	Data Domain DD160		
Manufacturer	EMC		
Serial number			
IP address			
Location	Dataplace B.V.		
	Van Coulsterweg 6, 2952 CB Alblasserdam		
	T.: (088) 328 27 52		
Power supply	- - -	Amount	1
Supplier	NedPortal		
	Londen 12, 2993 LA Barendrecht		
	T.: (088) 557 03 33		
Functionalities	• *Offsite backup*		

LH-SAN01			
Model	StorageWorks P4300 G2		
Manufacturer	HP		
Serial number			
Memory	8GB		
Disk space	7,2 TB	RAID configuration	RAID 5
		RAID network configuration	RAID 10 + 1
IP address			
Domain			
Location	Server room 1		
Power supply	750W	Amount	2
Supplier	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities	• *SAN Storage*		

LH-SAN02			
Model	StorageWorks P4300 G2		
Manufacturer	HP		
Serial number			
Memory	8 GB		
Disk space	7,2 TB	RAID configuration	RAID 5
		RAID network configuration	RAID 10 + 1
IP address			
Domain			
Location	Server room 2		
Power supply	750W	Amount	2
Supplier	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities	• *SAN Storage*		

LH-SAN03			
Model	StoreVirtual 4330		
Manufacturer	HP		
Serial number			
Memory	8 GB		
Disk space	7,2 TB	RAID configuration	RAID 5
		RAID network configuration	RAID 10 + 1
IP address			
Domain			
Location	Server room 1		
Power supply	460W	Amount	2
Supplier	NedPortal		
	Londen 12, 2993 LA Barendrecht		
	T.: (088) 557 03 33		
Functionalities	• *SAN Storage*		

LH-SAN04			
Model	StoreVirtual 4330		
Manufacturer	HP		
Serial number			
Memory	8 GB		
Disk space	7,2 TB	RAID configuration	RAID 5
		RAID network configuration	RAID 10 + 1
IP address			
Domain			
Location	Server room 2		
Power supply	460W	Amount	2
Supplier	NedPortal		
	Londen 12, 2993 LA Barendrecht		
	T.: (088) 557 03 33		
Functionalities	• *SAN Storage*		

VMWSRV01			
Model	ProLiant DL380p Gen8		
Manufacturer	HP		
Serial number			
Processor	2 x 8-Core 2GHz Intel Xeon CPU E5-2650 0 @ 2.00GHz		
Memory	96 GB		
Disk space	130 GB	RAID configuration	RAID 1
Operating System	VMware ESXi 5.1.0		
License code			
IP address			
Domain			
Location	Server room 1		
Power supply	750W	Amount	2
Backup location	EMCDD01		
Supplier	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities	• *Part of the VMware environment*		

VMWSRV02			
Model	ProLiant DL380p Gen8		
Manufacturer	HP		
Serial number			
Processor	2 x 8-Core 2GHz Intel Xeon CPU E5-2650 0 @ 2.00GHz		
Memory	96 GB		
Disk space	130 GB	RAID configuration	RAID 1
Operating System	VMware ESXi 5.1.0		
License code			
IP address			
Domain			
Location	Server room 2		
Power supply	750W	Amount	2
Backup location	EMCDD01		
Supplier	Unit4		
	Stationspark 1000, 3364 DA Sliedrecht		
	T.: (0184) 44 44 44		
Functionalities	• *Part of the VMware environment*		

Servers (VM)

ARSRV01			
Memory	8 GB		
Provisioned storage	60 GB		
Operating System	Microsoft Windows Server 2012		
IP address			
Domain			
Operates on server	VMWSRV01		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *Eagle Presence Registration*		

CRMSRV02			
Memory	4 GB		
Provisioned storage	50 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV01		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *Unit4 CRM*		

CTXSRV07			
Memory	8 GB		
Provisioned storage	80 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV01		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *Powerfuse 2012*		
	• *Citrix XenApp 6.5 Advanced Edition*		

DBSRV02			
Memory	4 GB		
Provisioned storage	90 GB		
Operating System	Microsoft Windows Server 2012		
IP address			
Domain			
Operates on server	VMWSRV01		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *Agresso Wholesale failover*		

DMNSRV02			
Memory	4 GB		
Provisioned storage	40 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV02		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *Domain Controller*		
	• *Safeword Token Database*		
	• *Domain related tasks*		
	• *Citrix License server*		
	• *Print server*		

ELOSRV01			
Memory	8 GB		
Provisioned storage	200 GB		
Operating System	Microsoft Windows Server 2012		
IP address			
Domain			
Operates on server	VMWSRV01		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *ELO Digital Archive*		

EXCSRV02			
Memory	15 GB		
Provisioned storage	200 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV01		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
	12 copies		Monthly *(last saturday of every month)*
Functionalities	• *Microsoft Exchange 2010*		

EXCSRV03			
Memory	15 GB		
Provisioned storage	200 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV02		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
	12 copies		Monthly *(last saturday of every month)*
Functionalities	• *Microsoft Exchange 2010*		

FRONTENDSRV01			
Memory	8 GB		
Provisioned storage	60 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV02		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
	12 copies		Monthly *(last saturday of every month)*
Functionalities	• *Connectivity mobile devices*		

PORTALSRV01			
Memory	4 GB		
Provisioned storage	40 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV01		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *DMZ*		
	• *Citrix XenApp Portal*		

RFSRV01			
Memory	8 GB		
Provisioned storage	80 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV01		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *RF system*		

SONICSRV01			
Memory	8 GB		
Provisioned storage	60 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV02		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *EDI Live Environment*		

SONICSRV02			
Memory	4 GB		
Provisioned storage	60 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV02		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *EDI Test Environment*		
	• *TopDesk*		

TLSSRV02			
Memory	8 GB		
Provisioned storage	160 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV02		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *McAfee Epolicy Orchestrator 5.1*		
	• *WSUS*		
	• *Veeam One Monitor*		

VEEAMSRV01			
Memory	4 GB		
Provisioned storage	40 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV02		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *Veeam 8.0*		

VPNSRV01			
Memory	8 GB		
Provisioned storage	60 GB		
Operating System	Microsoft Windows Server 2012		
IP address			
Domain			
Operates on server	VMWSRV01		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *Routing and Remote Access*		
	• *Safeword*		

VSPHERE01			
Memory	8 GB		
Provisioned storage	130 GB		
IP address			
Domain			
Operates on server	VMWSRV01		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily

WEBSRV03			
Memory	8 GB		
Provisioned storage	60 GB		
Operating System	Microsoft Windows Server 2008 R2		
IP address			
Domain			
Operates on server	VMWSRV02		
Backup location	EMCDD01		
Backup Retention	14 copies	Scheduled	Daily
Functionalities	• *DMZ*		
	• *Unit4 WebSolutions*		

Switches

HP ProCurve 2920-24G-PoE	
Model	ProCurve 2920-24G-PoE
Manufacturer	HP
Ethernet ports	*None*
Gigabit ports	24
VLAN	
IP address	
Domain	
Location	Server room 1
Supplier	LanTel
	Pieter Zeemanweg 57, 3316 GZ Dordrecht
	T.: (078) 630 55 55
Functionalities	• *Accesspoints from Aerohive WiFi are connected to this switch*

HP ProCurve Switch 4208VL	
Model	ProCurve 4208VL
Manufacturer	HP
Ethernet ports	164
Gigabit ports	20
VLAN	
IP address	
Domain	
Location	Server room 1
Supplier	Unit4
	Stationspark 1000, 3364 DA Sliedrecht
	T.: (0184) 44 44 44
Functionalities	• *Main switch (core switch)*

HP ProCurve Switch E3500YL-24G-PoE (LH-Switch_1)	
Model	ProCurve Switch E3500YL-24G-PoE
Manufacturer	HP
Ethernet ports	*None*
Gigabit ports	24
VLAN	
IP address	
Domain	
Location	Server room 1
Supplier	Unit4
	Stationspark 1000, 3364 DA Sliedrecht
	T.: (0184) 44 44 44
Functionalities	• *Part of the VMware environment*
	• *Part of Failover environment*
	• *Part of iSCSI Network*

HP ProCurve Switch E3500YL-24G-PoE (LH-Switch_2)	
Model	ProCurve Switch E3500YL-24G-PoE
Manufacturer	HP
Ethernet ports	*None*
Gigabit ports	24
VLAN	
IP address	
Domain	
Location	Server room 2
Supplier	Unit4
	Stationspark 1000, 3364 DA Sliedrecht
	T.: (0184) 44 44 44
Functionalities	• *Part of the VMware environment*
	• *Part of Failover environment*
	• *Part of iSCSI Network*

HP ProCurve Switch 2610-12/24 PWR	
Model	ProCurve 2610-12/24 PWR
Manufacturer	HP
Ethernet ports	28
Gigabit ports	2
VLAN	
IP address	
Domain	
Location	Server room 1
Supplier	Actemium
	Industrielaan 18 (Postbus 169), 6950 AD Dieren
	T.: (0313) 43 01 11
Functionalities	• *Part of the RF environment*

Motorola RFS6000 Primary	
Model	RFS6000
Manufacturer	Motorola
Ethernet ports	*None*
Gigabit ports	8
VLAN	
IP address	
Domain	
Location	Server room 1
Supplier	Actemium
	Industrielaan 18 (Postbus 169), 6950 AD Dieren
	T.: (0313) 43 01 11
Functionalities	• *Controller for WiFi Accesspoints RF*

Motorola RFS6000 Secondary	
Model	RFS6000
Manufacturer	Motorola
Ethernet ports	*None*
Gigabit ports	8
VLAN	
IP address	
Domain	
Location	Server room 1
Supplier	Actemium
	Industrielaan 18 (Postbus 169), 6950 AD Dieren
	T.: (0313) 43 01 11

Router

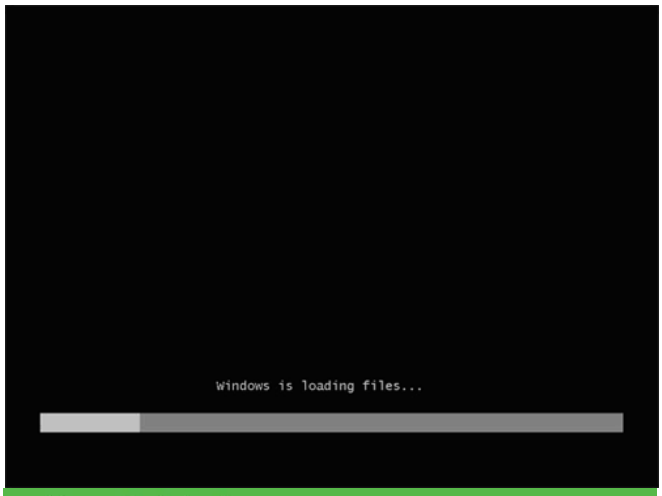
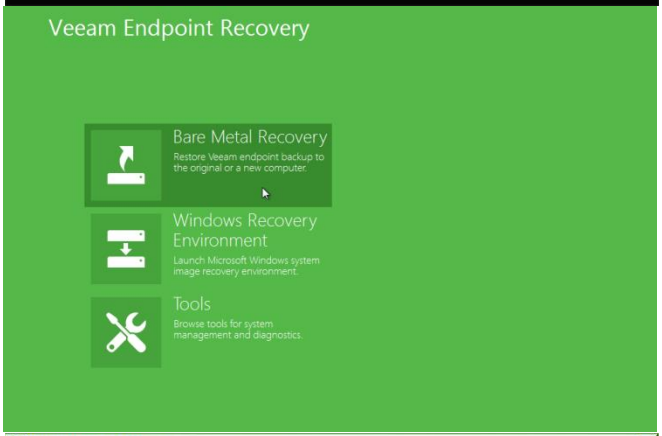
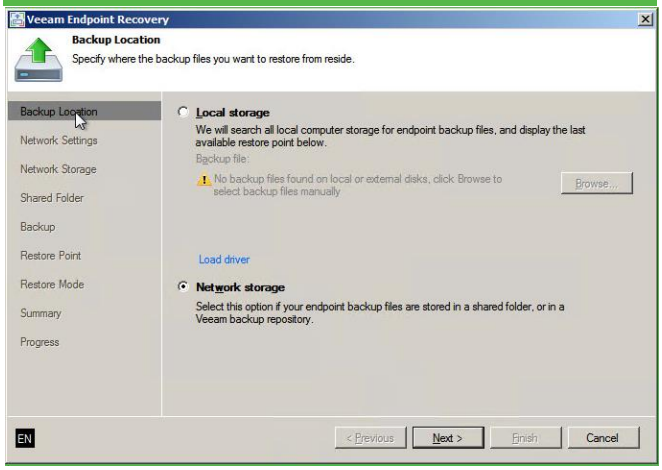
Cisco C8536	
Model	C8536
Manufacturer	Cisco
Location	Server room 1
Supplier	KPN
Functionalities	• *Internet connection*

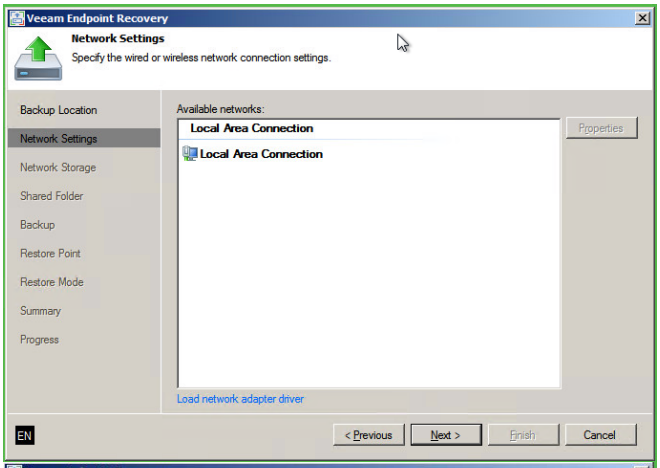
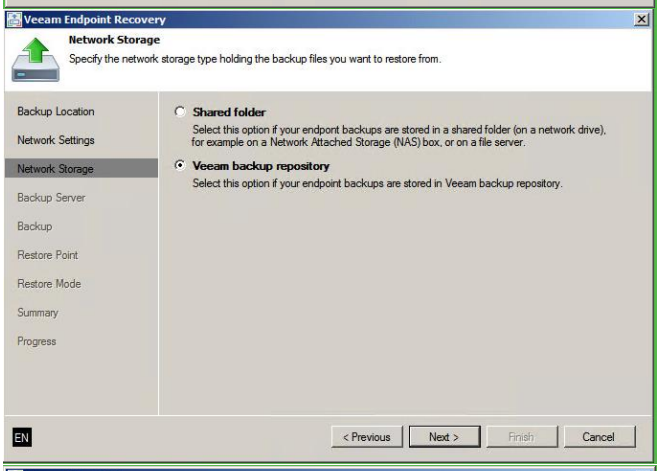
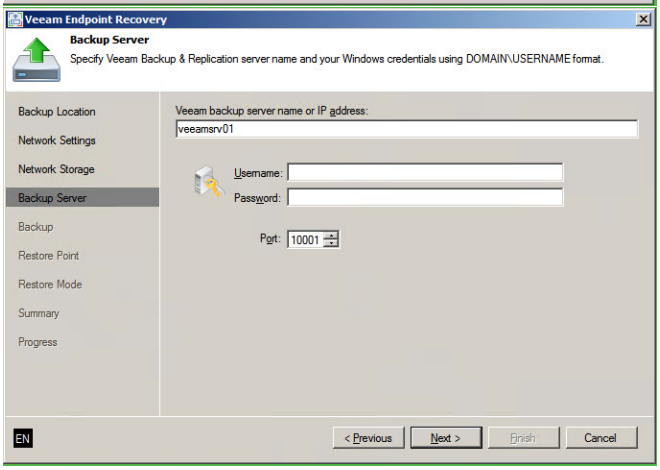
Firewall

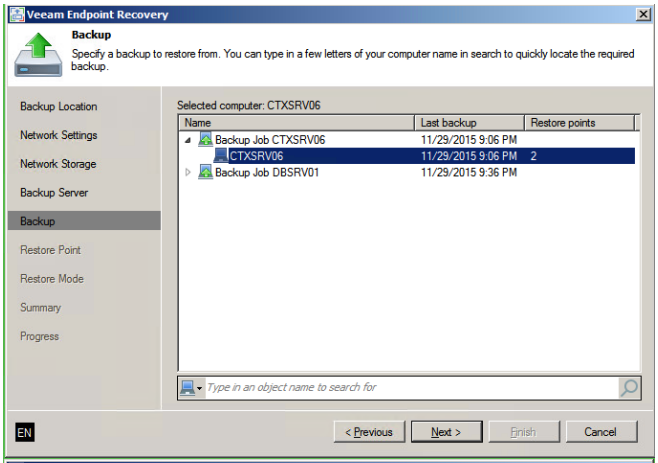
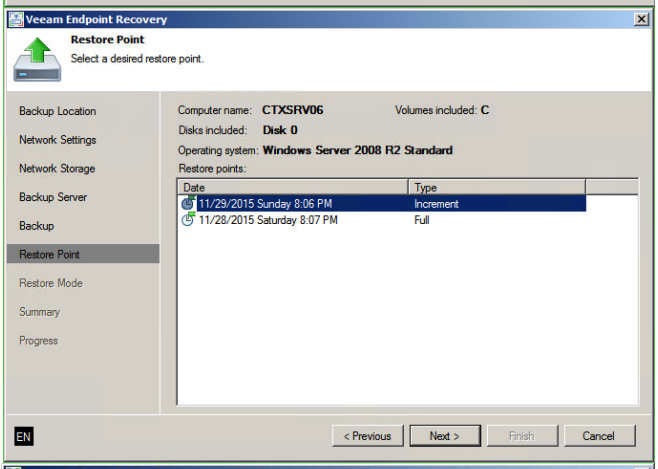
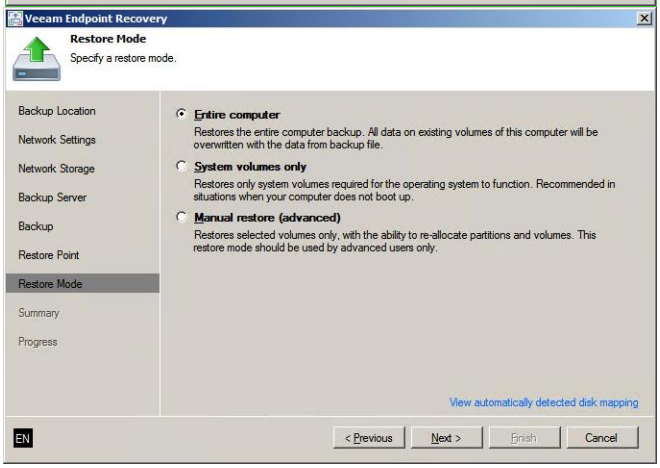
Juniper SSG140	
Model	SSG140
Manufacturer	Juniper
Port 0/0	
Port 0/2	
Port 0/6	
Port 0/7	
IP address	
Domain	
Location	Server room 1
Supplier	Unit4
	Stationspark 1000, 3364 DA Sliedrecht
	T.: (0184) 44 44 44
Functionalities	• *Gateway*
	• *VPN TUK*
	• *VPN TDEG*

Appendix C - IT system restore procedures

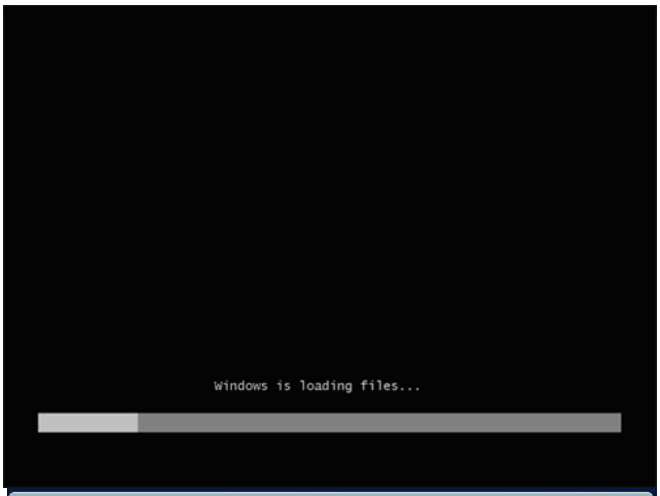
Servers (physical)

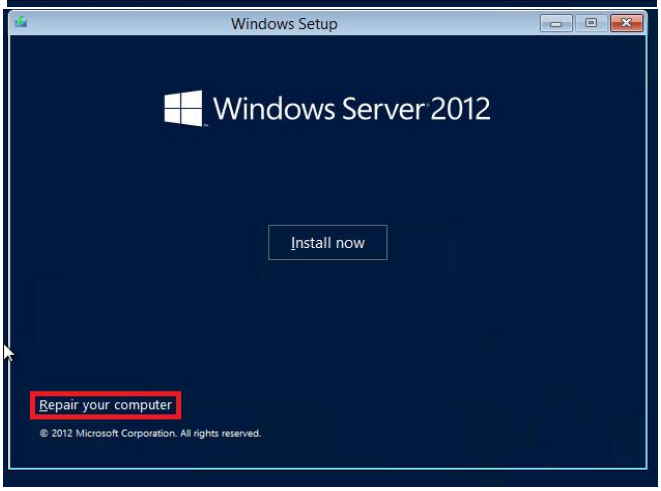
CTXSRV06 (Veeam Endpoint Recovery)	
1	Insert "Veeam Recovery Media CTXSRV06" CD
2	Boot from CD 
3	Launch the **Veeam Endpoint Recovery** Wizard In the **Veeam Endpoint Recovery** menu, select "Bare Metal Recovery" 
4	In the **Backup Location menu**, select "Network Storage" 

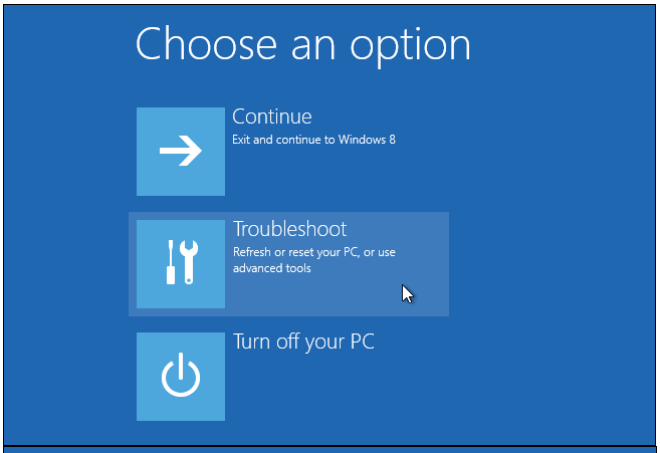
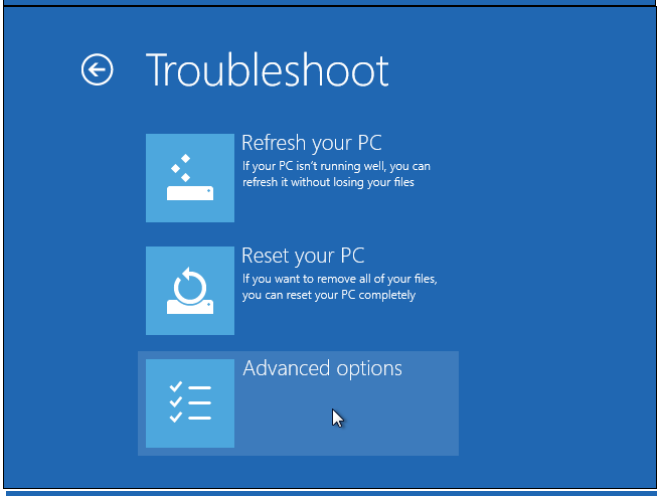
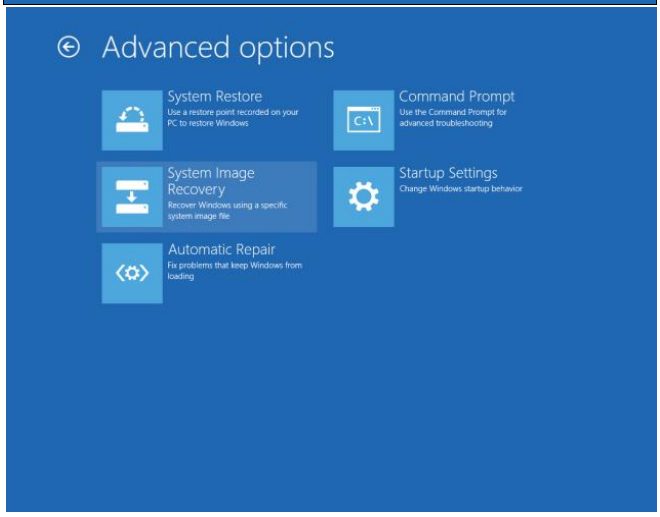
5	In the **Network Settings** menu, check the Local Area Connection settings and click on "Next"	
6	In the **Network Storage** menu, select "Veeam backup repository"	
7	In the **Backup Server** menu, type the: Veeam backup server name or IP address: Port: 10001	

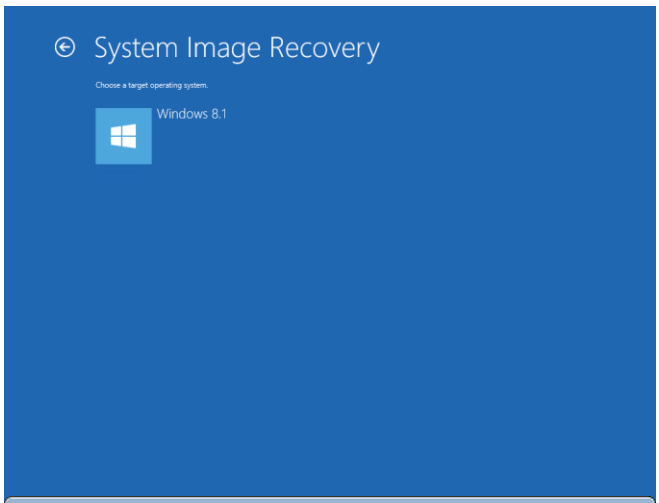
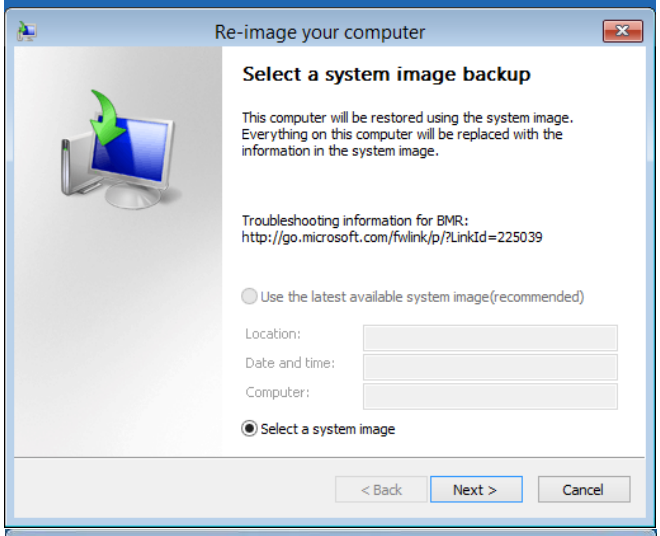
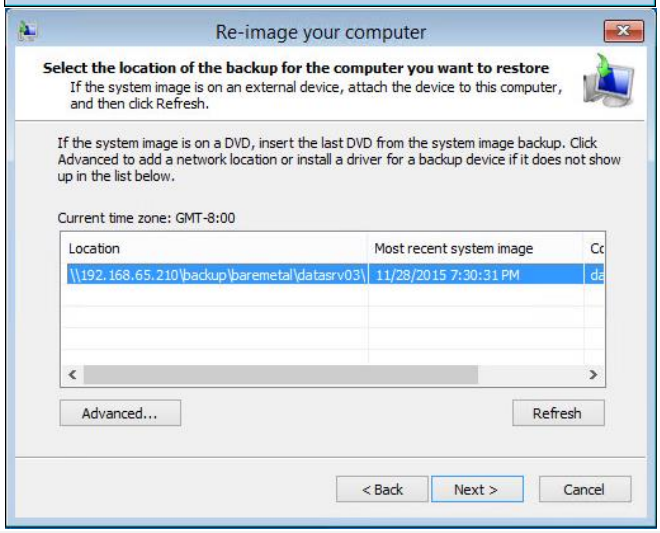
8	In the **Backup** menu, select a backup to restore from Selected computer: **CTXSRV06** Backup job: **CTXSRV06**	
9	In the **Restore Point** menu, select an Increment or Full Backup	
10	In the **Restore Mode** menu, select "Entire computer" to restore an entire computer backup	
11	At the **Summary** step, finalize the recovery process *Review the specified recovery settings in the previous steps, and click* **Restore** *to start the recovery process*	
12	When the recovery process finished successfully, restart the system	

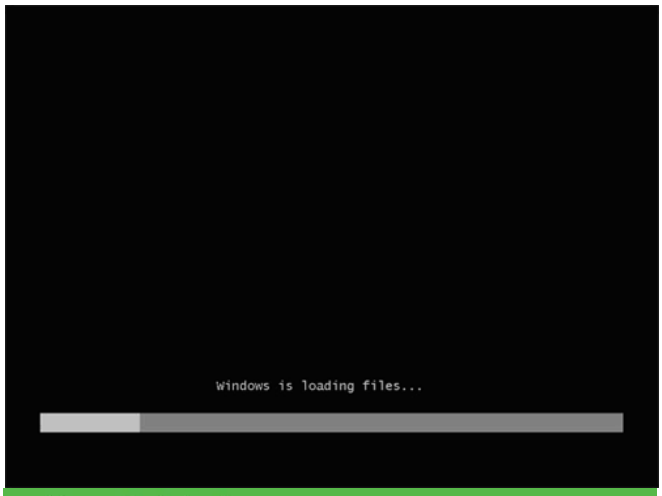
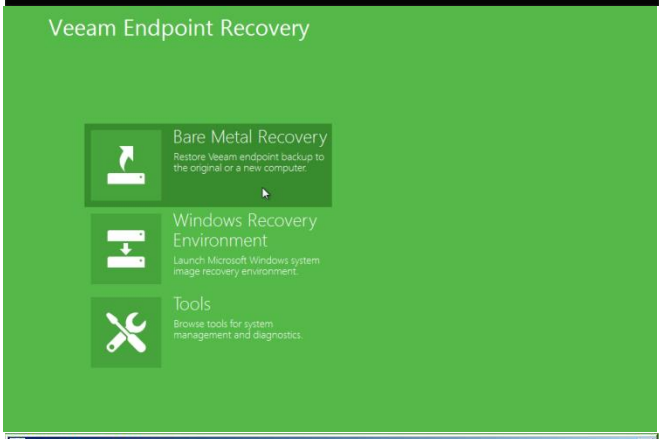
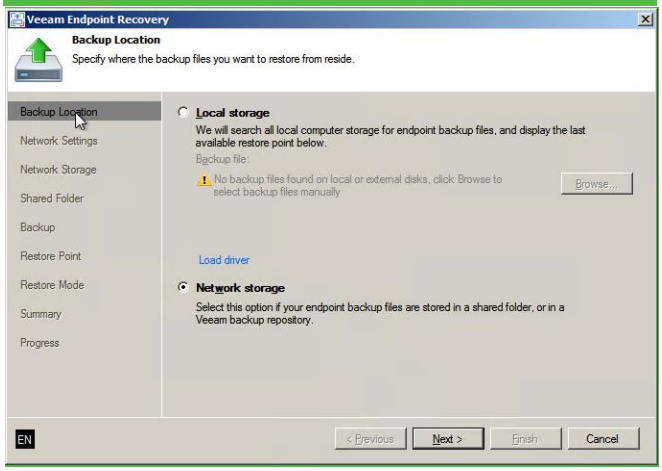
DATASRV03 (Windows Backup)	
1	Insert "System Recovery Disk DATASRV03" CD
2	Boot from CD
3	The **Windows Setup** will be launched. Check the language settings and click on "Next"
4	In the **Windows Setup** window, select "Repair your computer"

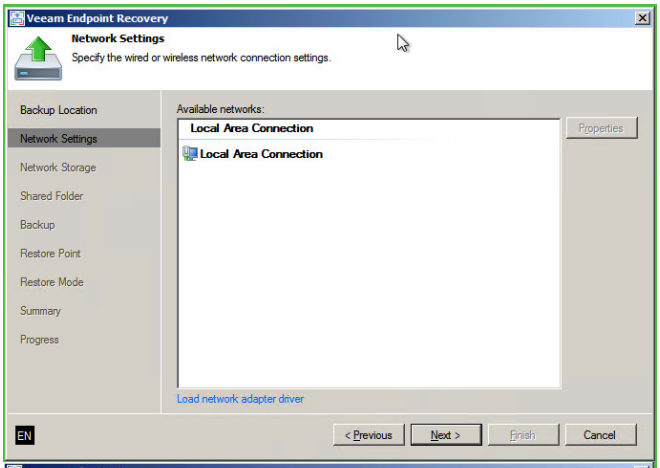
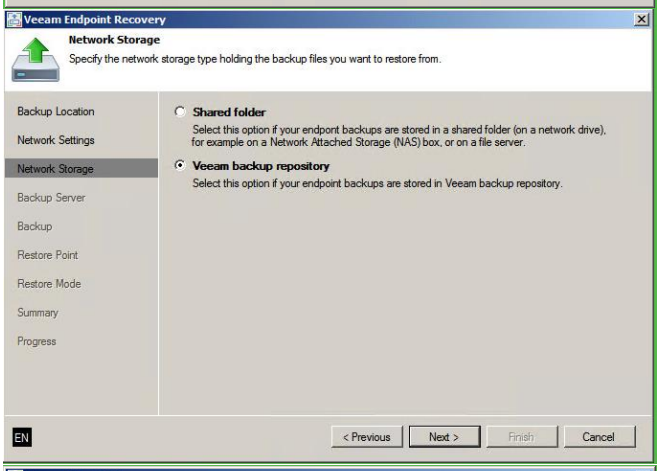
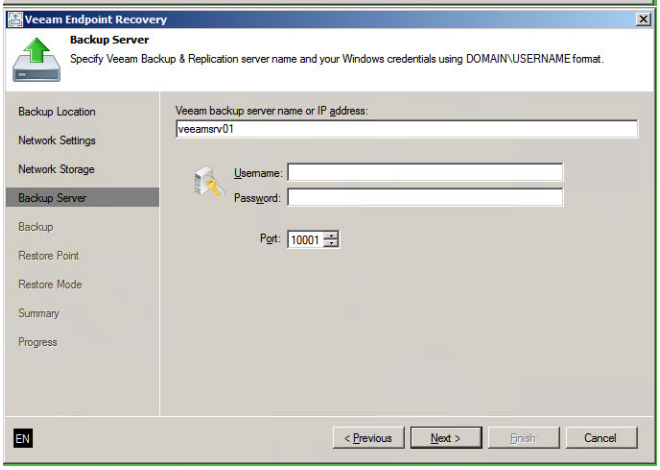


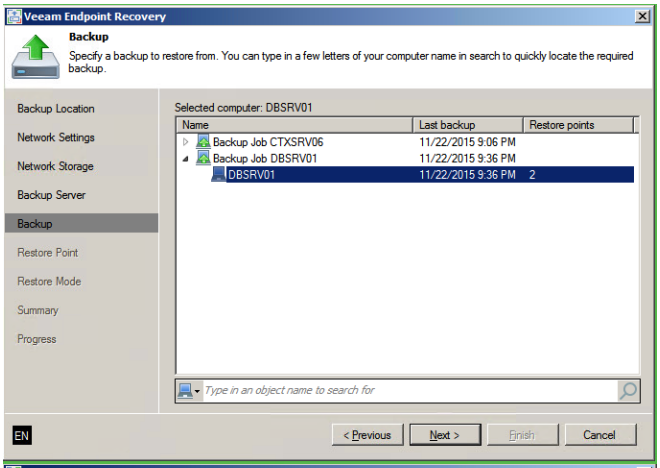
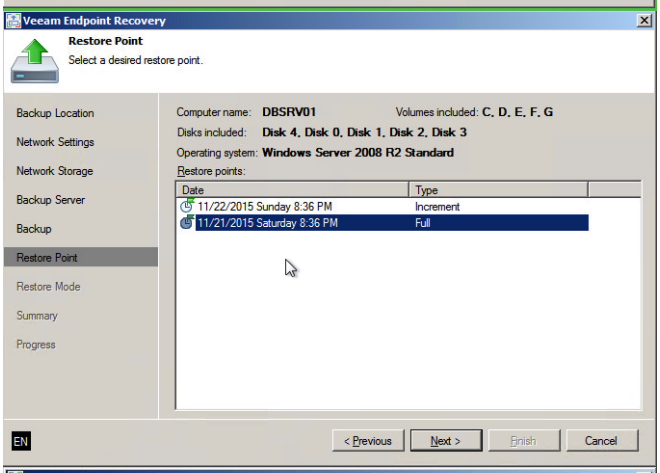
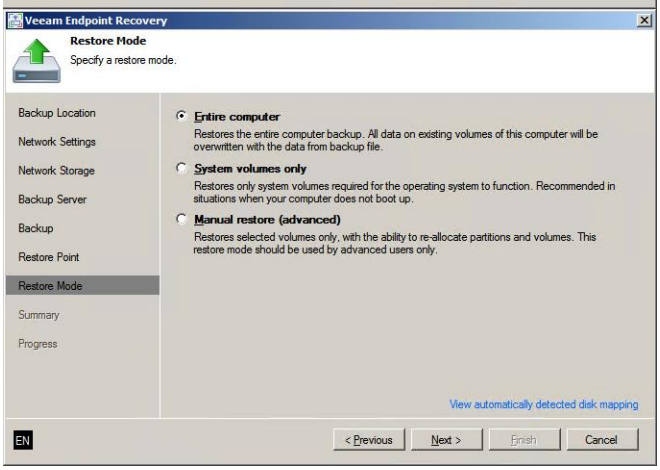


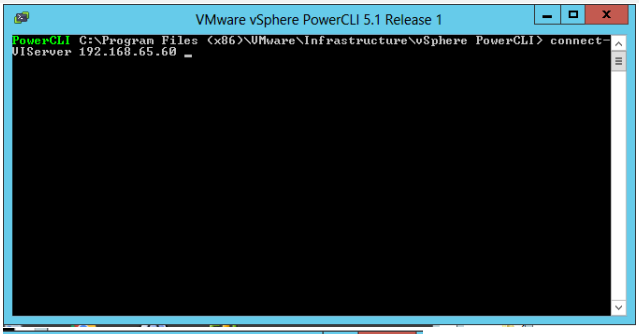
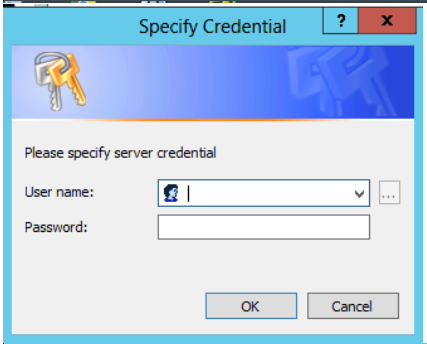
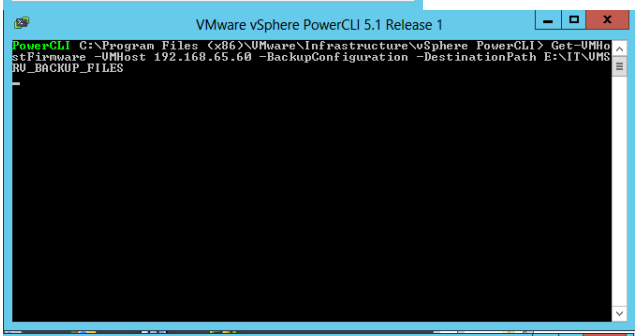
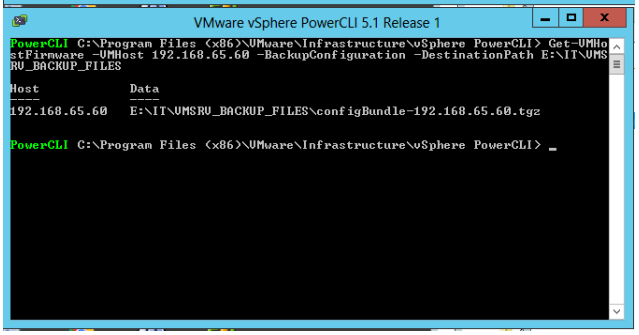
5	In the **Choose an option** menu, select "Troubleshoot"	
6	In the **Troubleshoot** menu, select "Advanced options"	
7	In the **Advanced options** menu, select "System Image Recovery"	

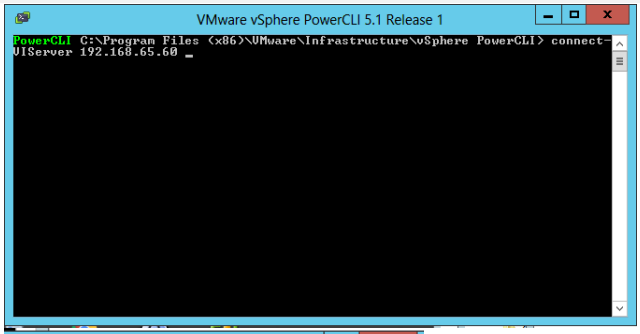
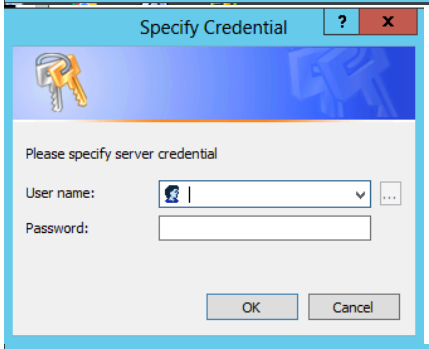
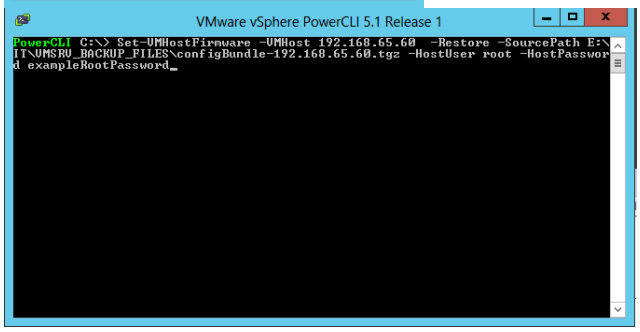
7	In the **System Image Recovery** menu, choose a target operating system. Select "Microsoft Windows Server 2008"	
8	In the **Re-image your computer** menu (under *Select a system image backup*), select "Select a System Image"	
9	In the **Select the location of the backup for the computer you want to restore** menu, click "Advanced". Next, select "Search for a system..." Select "Re-image your computer" Network folder: Enter network username and password to connect to	
10	Summary checkup and click "Finish". Select "Yes" to format and replace.	

DBSRV01 (Veeam Endpoint Recovery)	
1	Insert "Veeam Recovery Media DBSRV01" CD
2	Boot from CD 
3	Launch the **Veeam Endpoint Recovery** Wizard. In the **Veeam Endpoint Recovery** menu, select "Bare Metal Recovery" 
4	Specify the **Backup Location** where the backup files you want to restore reside. Select "Network storage" 

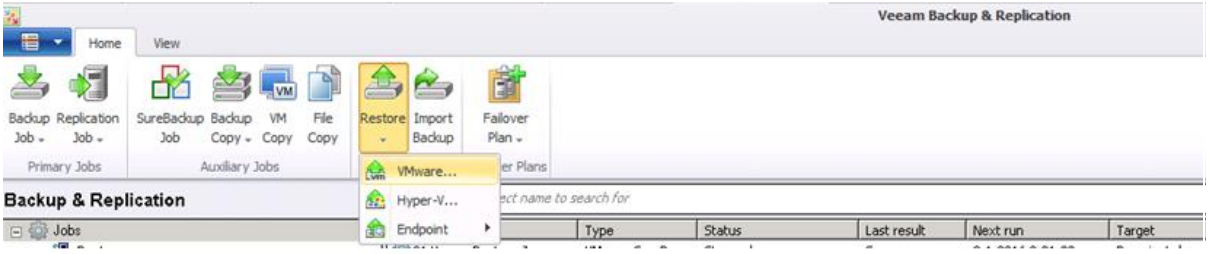
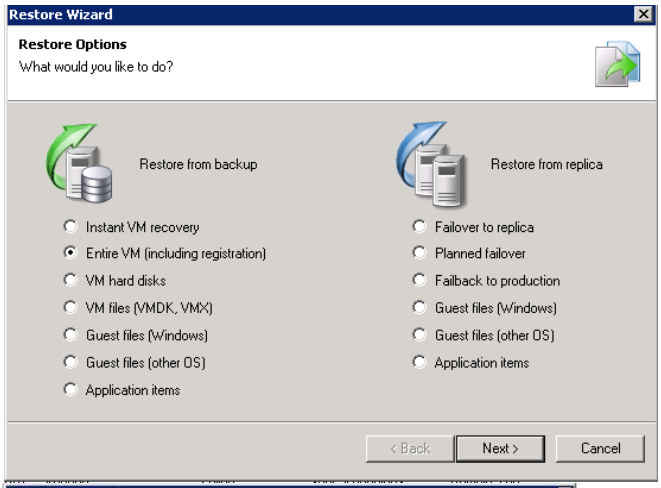
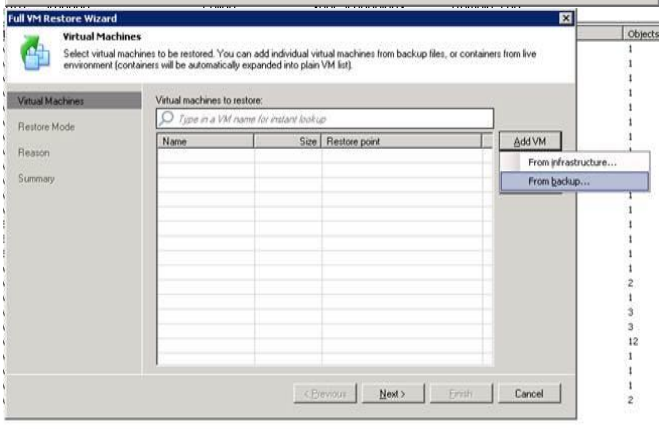
5	Specify the **Network Settings** Under "Local Area Connection", select "Local Area Connection"	
6	Specify the **Network Storage** type holding the backup files you want to restore from. Select "Veeam backup repository"	
7	Specify the **Backup Server** Veeam backup server name or IP address: Port: 10001	

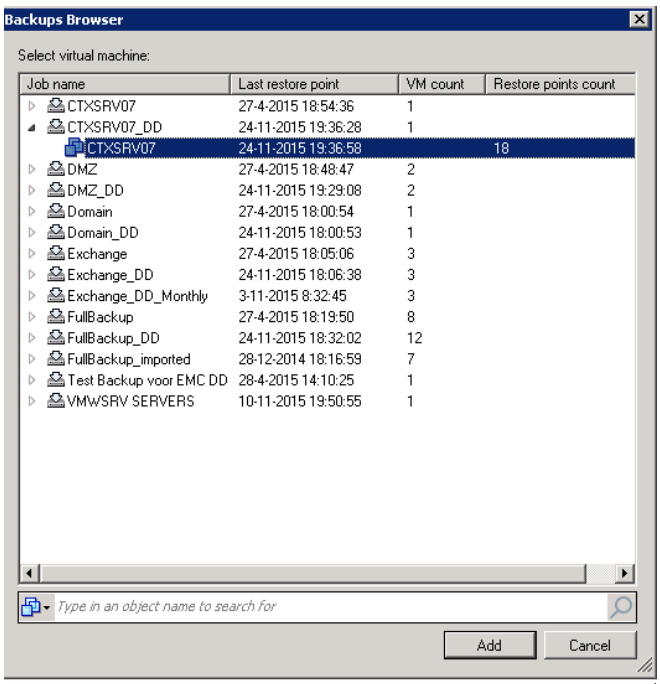
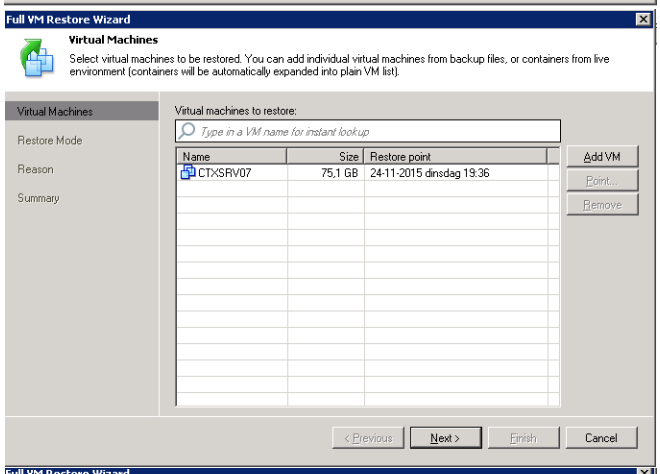
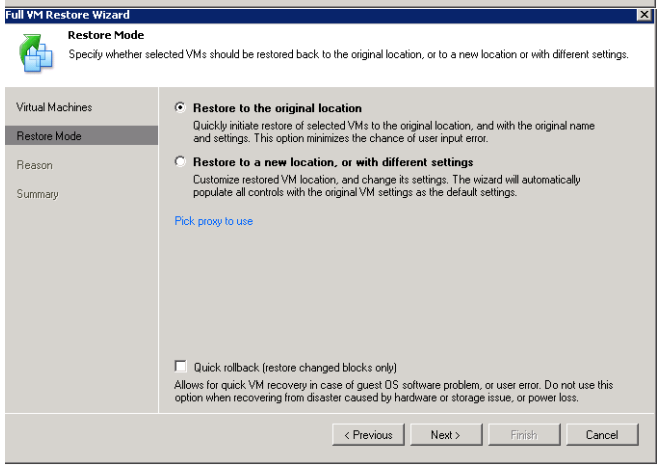
8	Specify a **Backup** to restore from. Selected computer: **DBSRV01** Backup job: **DBSRV01**	
9	Specify a **Restore Point** Select an Increment or Full Backup	
10	Specify **Restore Mode** Select "Entire computer" to restore an entire computer backup	
11	At the **Summary** step, finalize the recovery process. *Review the specified recovery settings in the previous steps, and click* **Restore** *to start the recovery process*	
12	When the recovery process finished successfully, restart the system.	

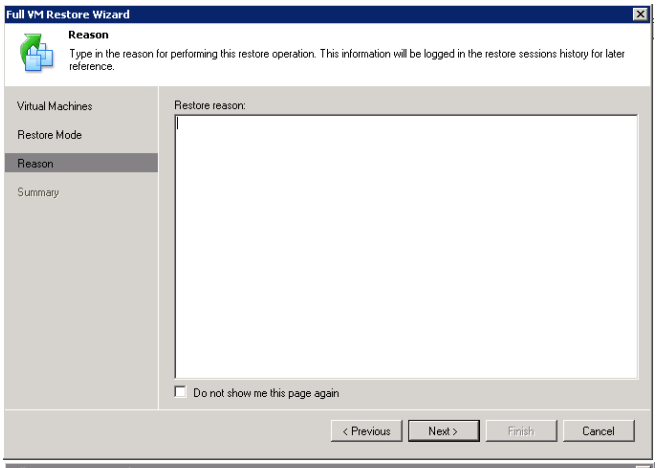
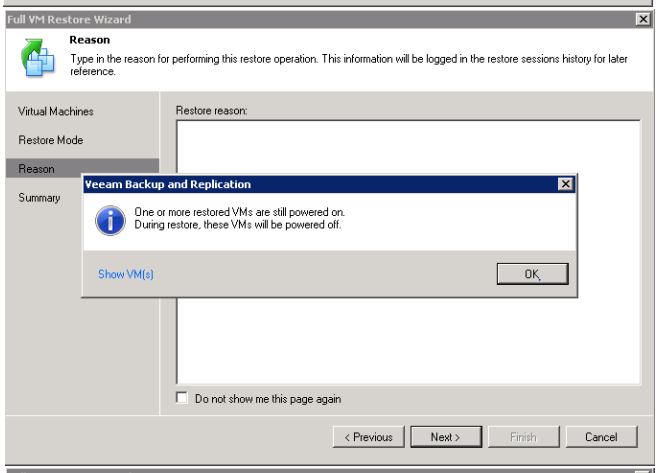
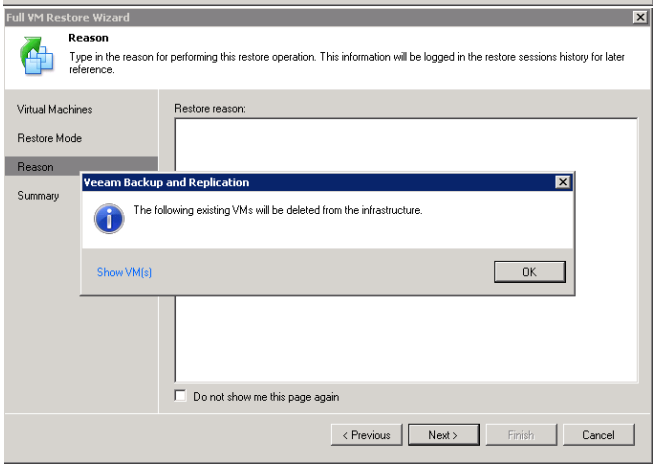
VMWSRV02 (vSphere PowerCLI)	
1	To back up the configuration data for an ESXi host, run this command: **Get-VMHostFirmware -VMHost *ESXi_host_IP_address* -BackupConfiguration -DestinationPath *output_directory*** **Note**: *"ESXi_host_IP_address"* is the IP address of the ESXi host and *"output_directory"* is the name of the directory where the output file will be created. A backup file is saved in the directory specified with the "-DestinationPath" option.
2	Start the VMWare vSphere PowerCLI
3	Run the following command: 
4	Specify the server credentials and Log in 
5	Run the following command to backup the configuration data: 
6	When the backup completed successfully, the following screen will be displayed: 

VMWSRV02 (vSphere PowerCLI)	
1	To restore the configuration from the backup bundle, run this command: **Set-VMHostFirmware -VMHost *ESXi_host_IP_address* -Restore -SourcePath *backup_file* -HostUser *username* -HostPassword *password***. **Note**: *"ESXi_host_IP_address"* is the IP address of the ESXi host, *backup_file* is the name of the backup bundle to use for the restore, and *username* and *password* are the credentials to use when authenticating with the host.
2	Start the VMWare vSphere PowerCLI
3	Run the following command: 
4	Specify the server credentials and Log in 
5	Run the following command to restore the configuration data: 

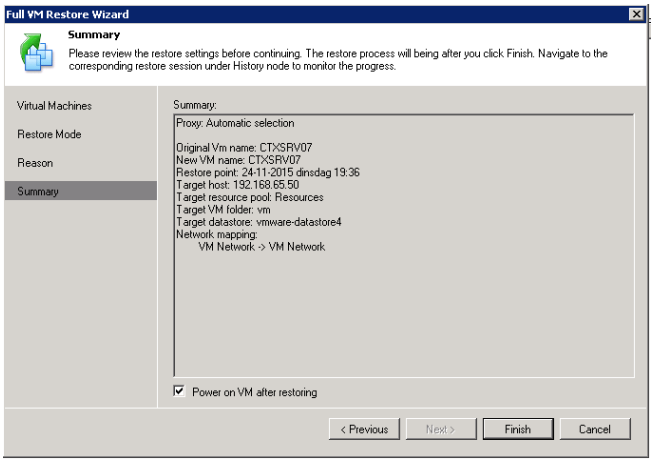
Servers (VM)

CTXSRV07 (Veeam Backup & Replication)	
1	Start an RDP session to the "veeamsrv01" server and Log in
2	Open "Veeam Backup & Replication"
3	In the **Veeam Backup & Replication** menu, click on "Restore" and click on "VMware..." 
4	In the **Restore Options** menu, under *Restore from backup*, select "Entire VM (including registration)" 
5	In the **Virtual Machines** menu, click on "Add VM" and click on "From backup..." 

6	In the **Backup Browser** menu, select a virtual machine (restore point) under "Job name" and click on "Add" ***** *Job names including '_DD' are restore points on our data domain*	
7	When the selected virtual machine appears in the **Virtual Machines** menu, click on "Next"	
8	In the **Restore Mode** menu, select "Restore to the original location"	

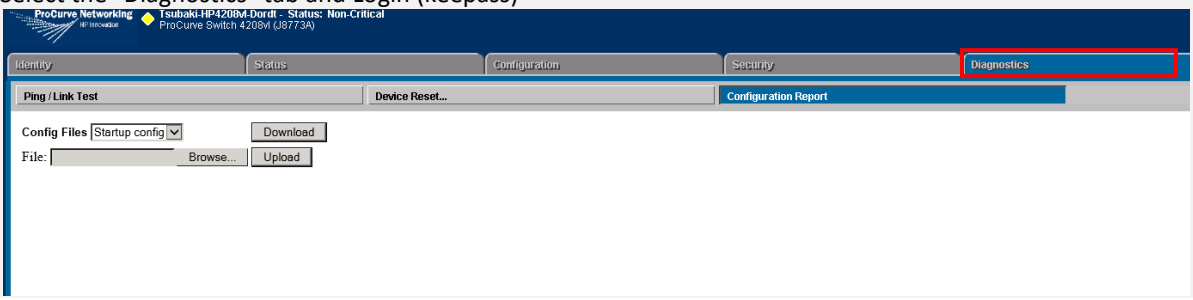
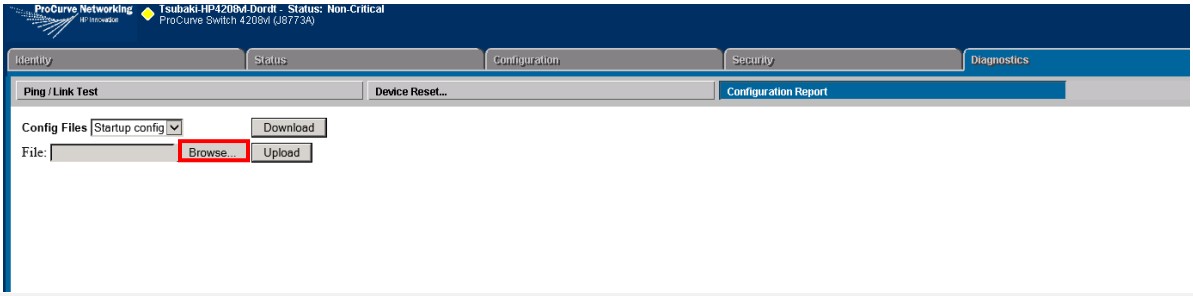
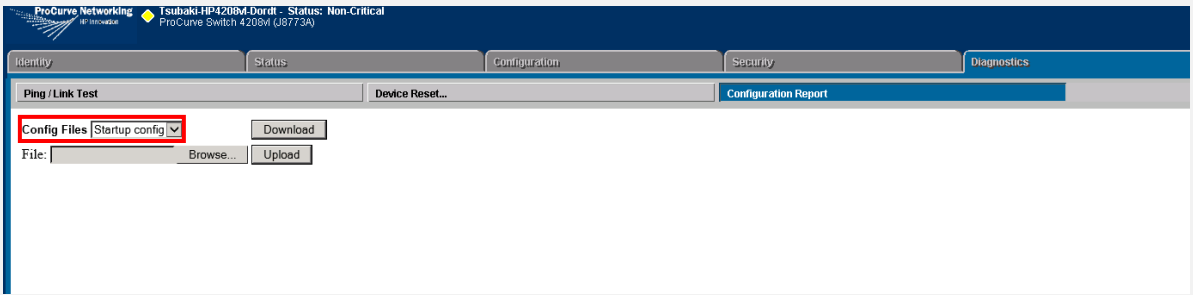
9	*Optional*: in the **Reason** menu, it is possible to specify a Restore reason and other additional information	
10	In case the virtual machine is still running, the following message will appear: *'One or more restored VMs are still powered on. During restore, these VMs will be powered off*.' Click on "Show VM(s)" to show these VMs ***** *These VMs will be powered off during restore* To continue, click on "OK"	
11	If the virtual machine is available in the infrastructure, the following message will appear: '*The following existing VMs will be deleted from the infrastructure*.' Click on "Show VM(s)" to show these VMs To continue, click on "OK"	

12	In the **Summary** menu, a summary of the restore is displayed. Select "Power on VM after restoring" and click on "Finish" *The restore will now start and boot the virtual machine from the backup*.

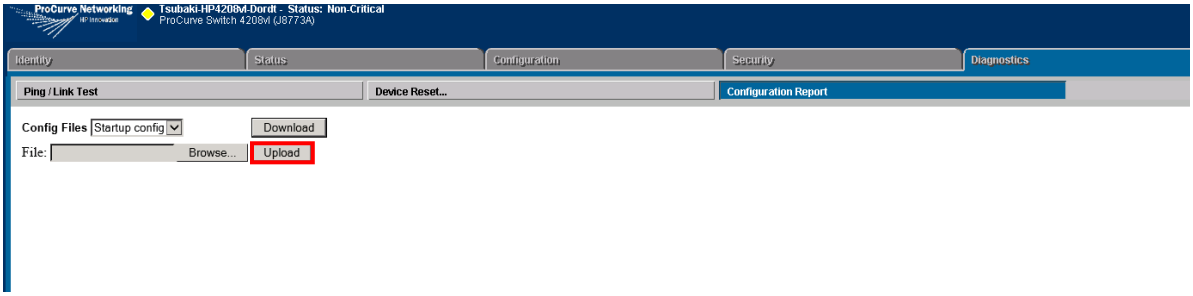


Switches

HP ProCurve 4208VL

1	Access the web GUI of the HP Switch
2	Select the "Diagnostics" tab and Login (keepass) 
3	Click on "Browse" and navigate to 
4	Choose the config file and click on "Open" 

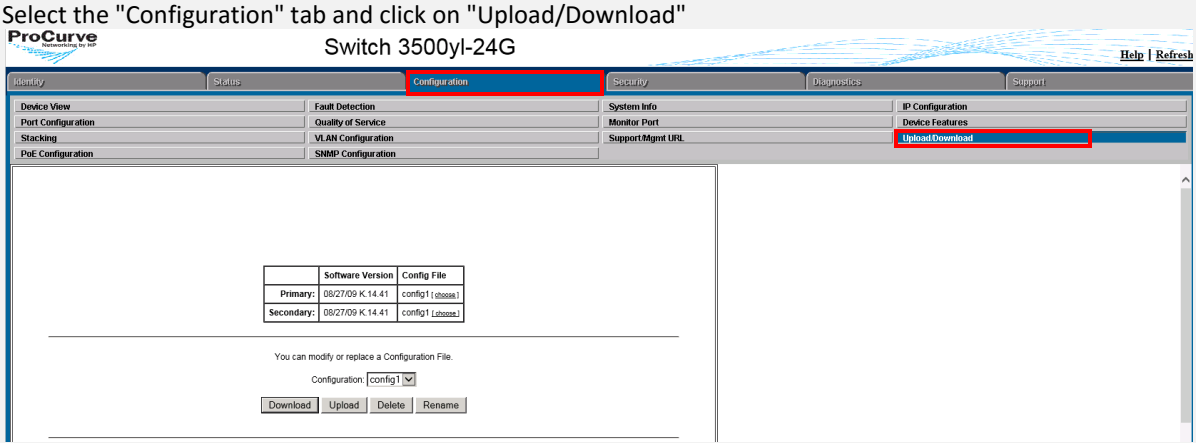
5 To finish, click on "Upload"



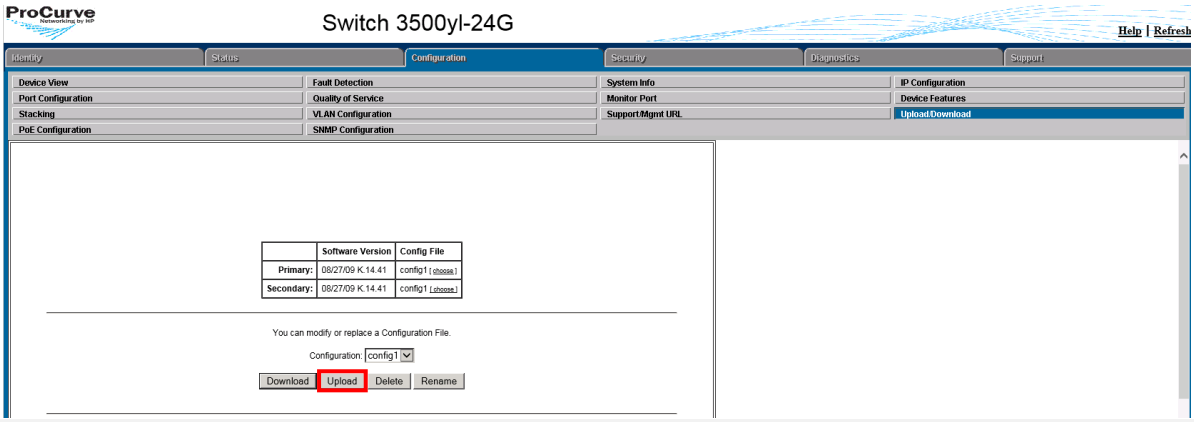
HP ProCurve E3500 YL-24G-PoE [1]

1 Access the web GUI of the HP Switch

2 Select the "Configuration" tab and click on "Upload/Download"

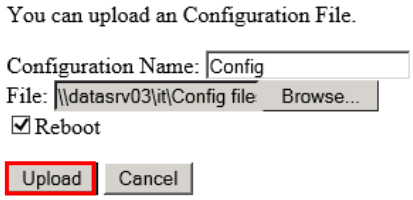


3 Click on "Upload" and navigate to



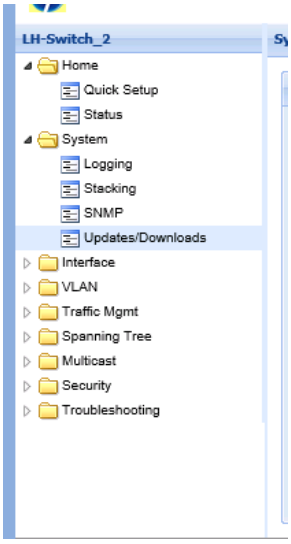
4 Select the config file and click on "Open"

5	To finish, click on "Upload"

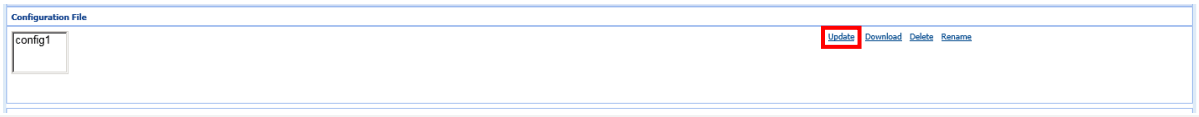


HP ProCurve E3500 YL-24G-PoE [2]

1	Access the web GUI of the HP Switch
2	Navigate to: - System -->: - Updates/Downloads



3	Click on "Update" and navigate to

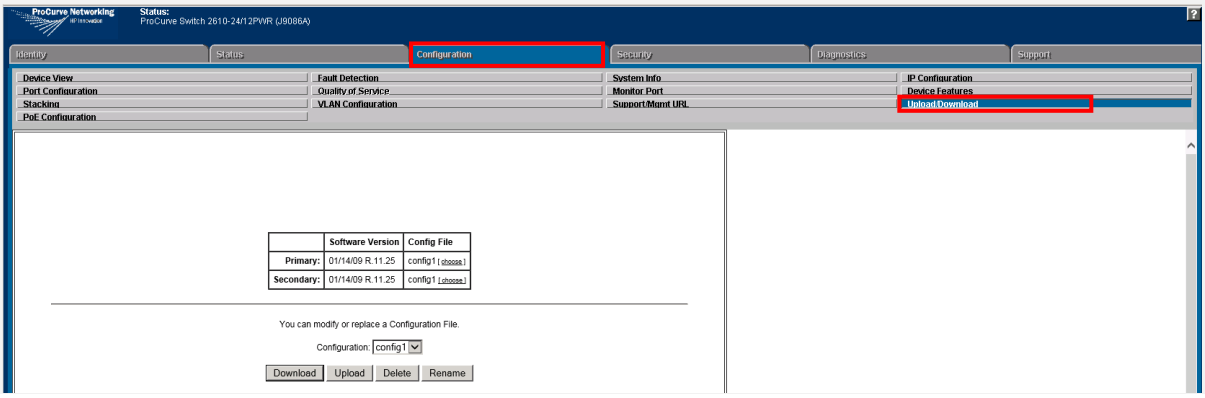


4	Select the config file and click on "Open"
5	To finish, click on "Save"

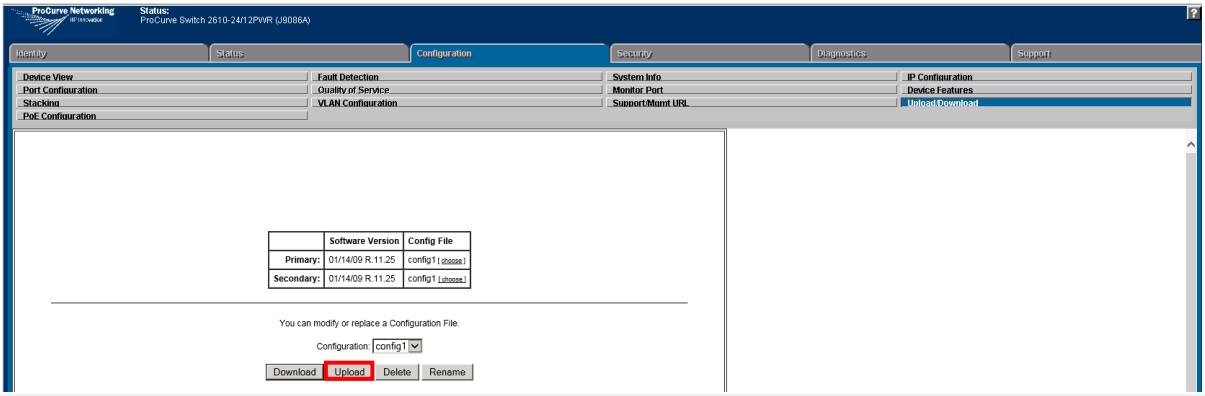
HP ProCurve 2610-12/24 PWR

1 Access the web GUI of the HP Switch

2 Select the "Configuration" tab and click on "Upload/Download"

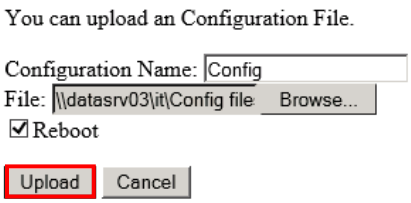


3 Click on "Upload" and navigate to

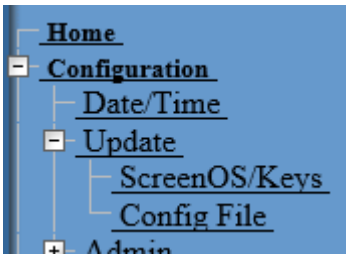
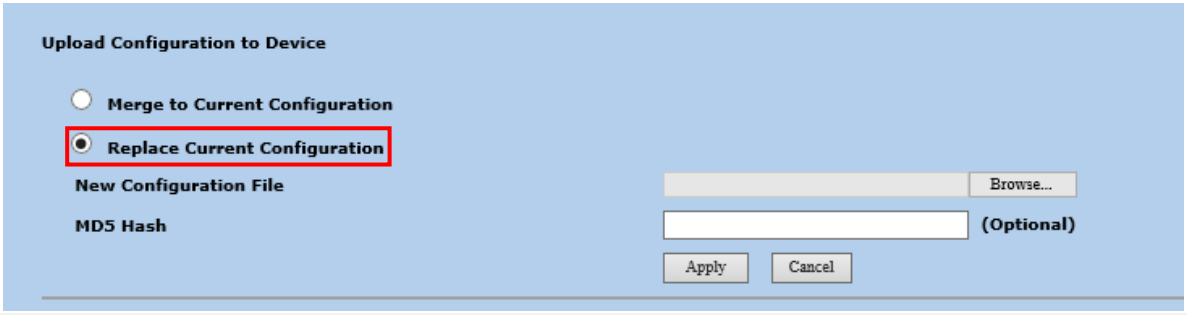
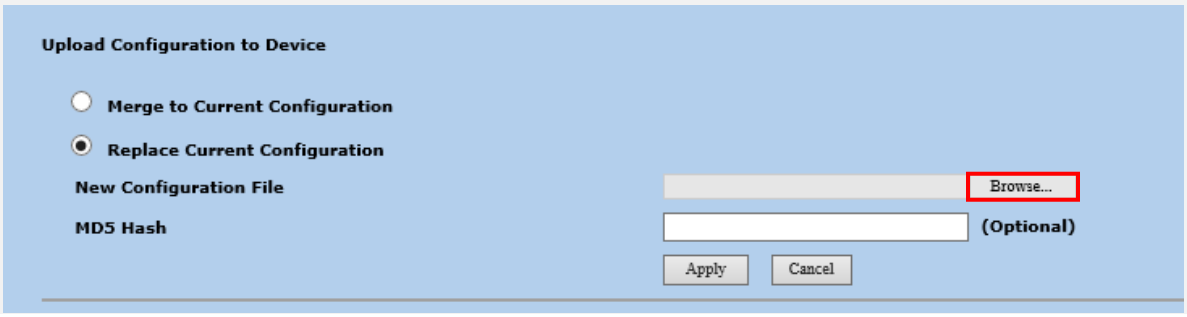
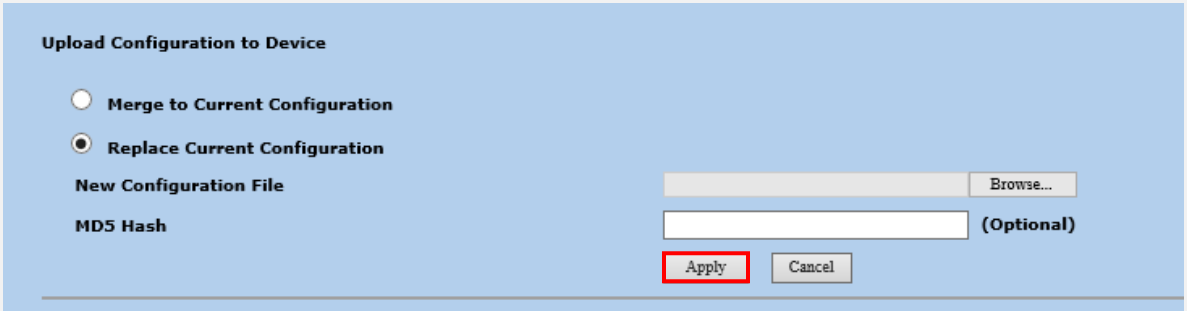


4 Select the config file and click on "Open"

5 To finish, click on "Upload"



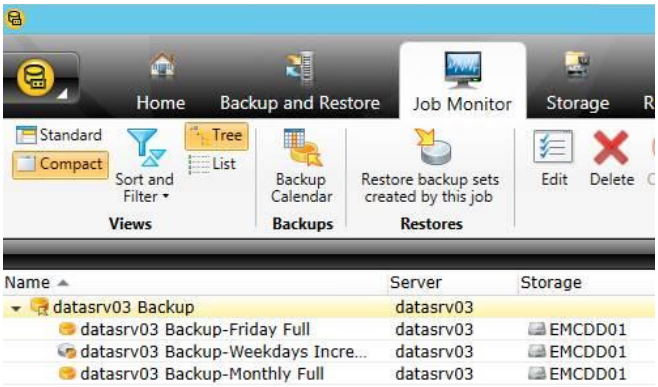
Firewall

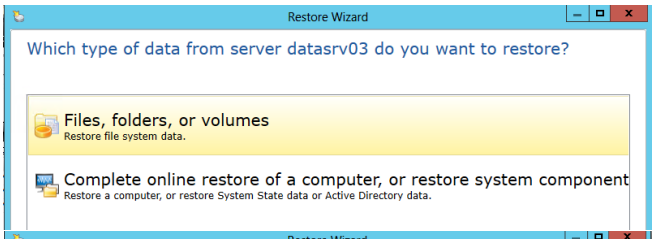
Juniper SSG140	
1	Access the web GUI of the Juniper Firewall
2	Navigate to: - Configuration -->: - Update -->: - Config File 
3	Select "Replace Current Configuration" 
4	Click on "Browse" and navigate to 
5	Navigate to ... and select the required config file
6	Click on "Open" and click on "Apply" 

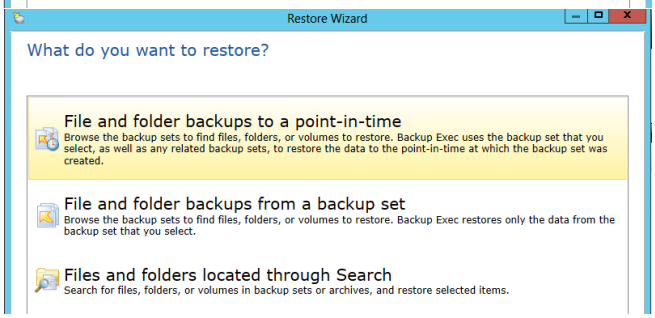
Appendix D - File restore procedure

File Restore Procedure

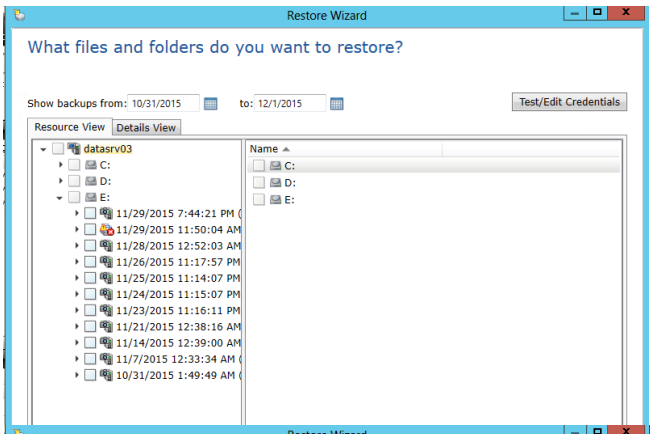
DATASRV03 (Symantec Backup Exec 2014)	
1	Open 'Symantec Backup Exec 2014' on DATASRV03
2	Click on the "Job Monitor" tab and select 'datasrv03 Backup' Above **Restores**, click on "Restore backup sets created by this job"
3	In the **Restore Wizard** menu, select "Files, folders, or volumes"
4	Next, in the **Restore Wizard** menu, select "File and folder backups to a point-in-time"

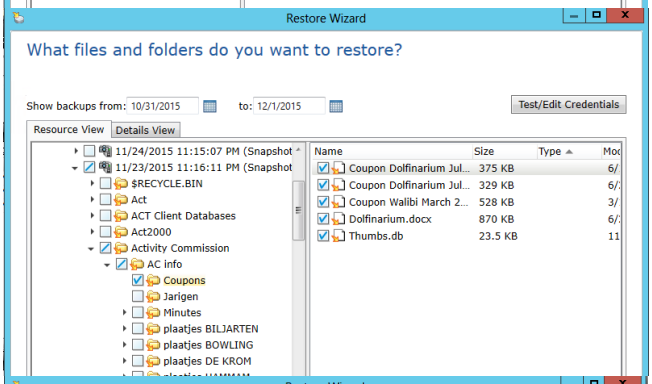


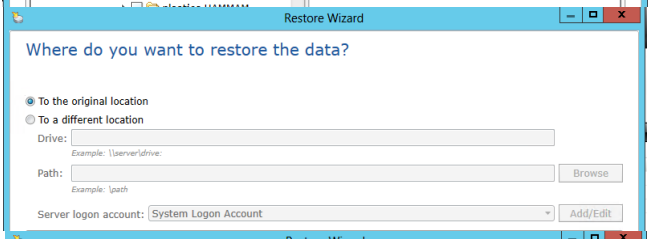


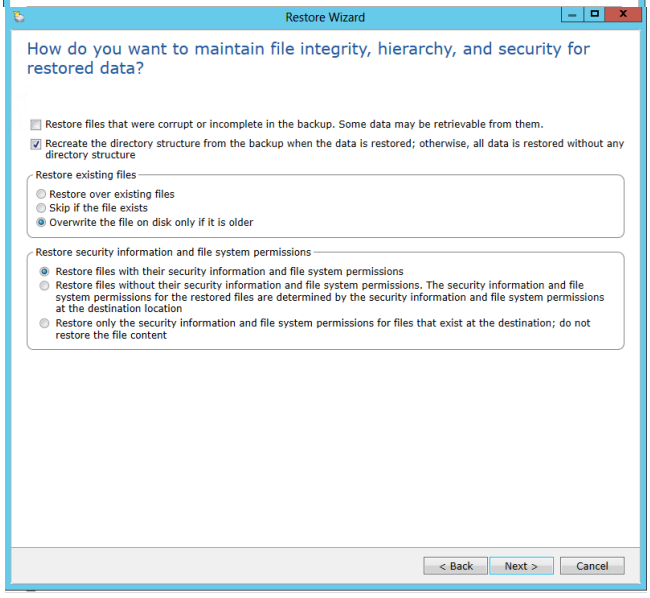


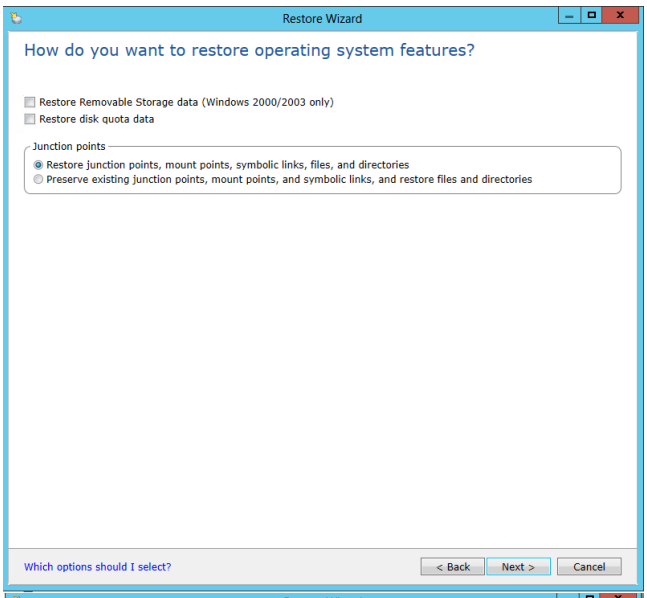
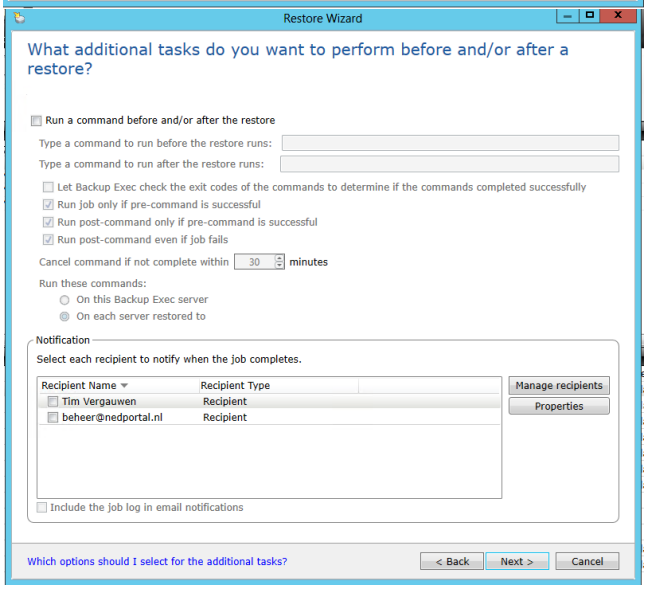
5	Select which files and folders you want to restore
6	In the "Show backups from:" section, a larger time window can be selected to find the right backup Click down the folder tree to find the files you want to restore
7	Select the location from where the data needs to be restored Click on "To the original location" ("To a different location" is also possible if you want to review the files first)
8	Make sure these settings are selected:



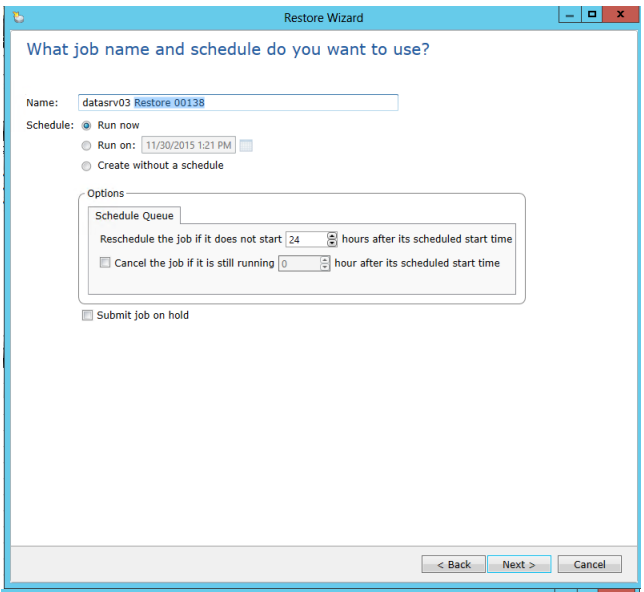




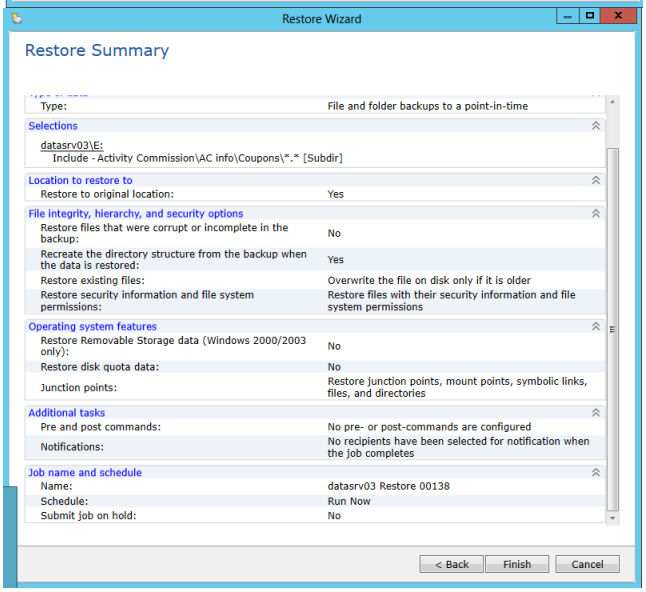


9	Under 'Junction points', select "Restore junction points, mount points, symbolic links, files, and directories"	
10	Here it is possible to select any additional tasks to be performed before and/or after a restore	

11	Specify a job name and schedule options

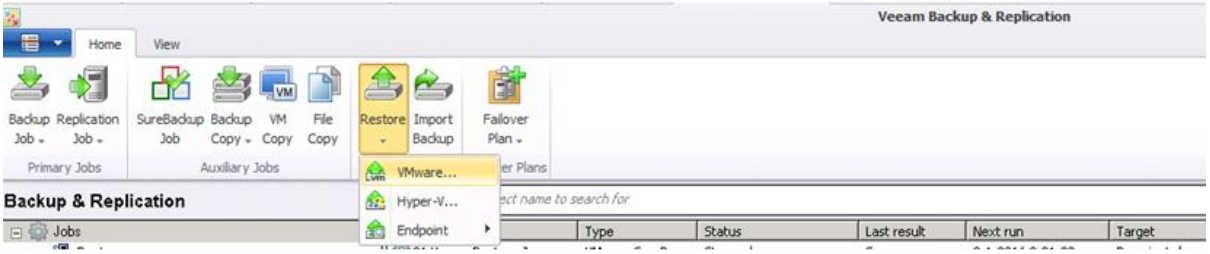
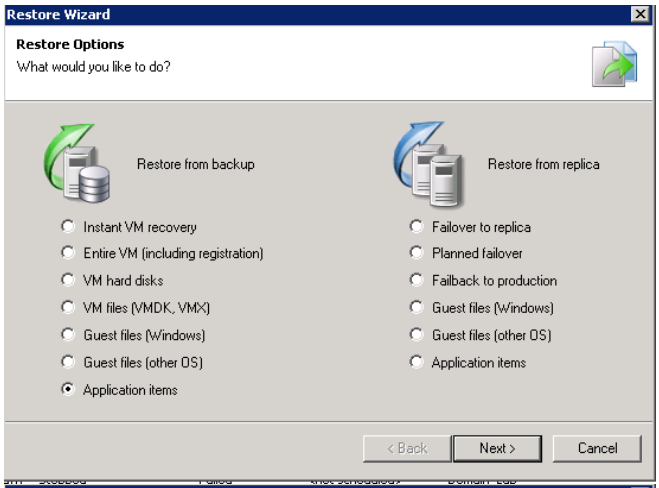
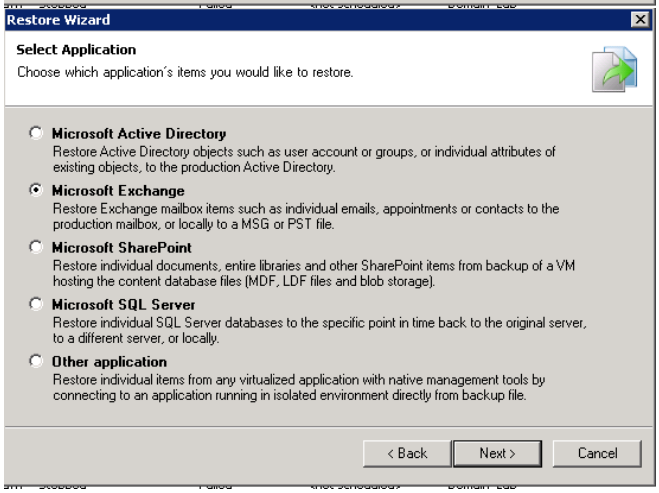


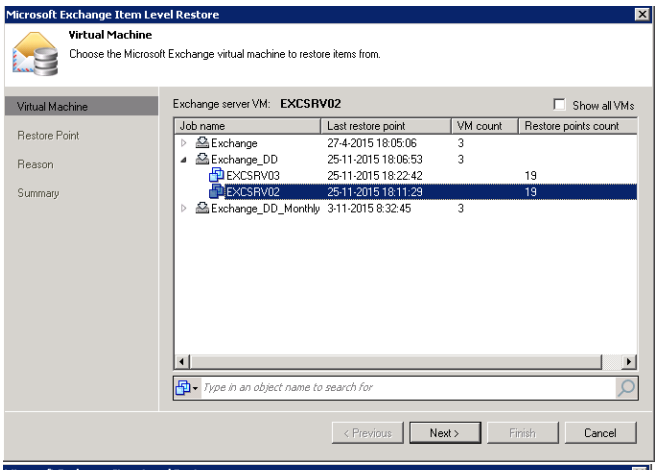
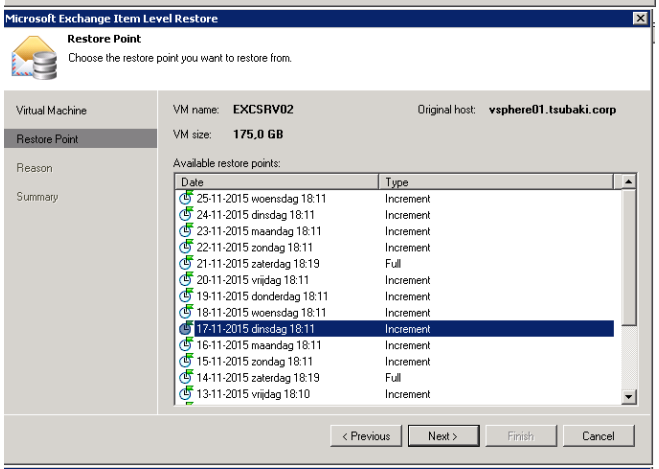
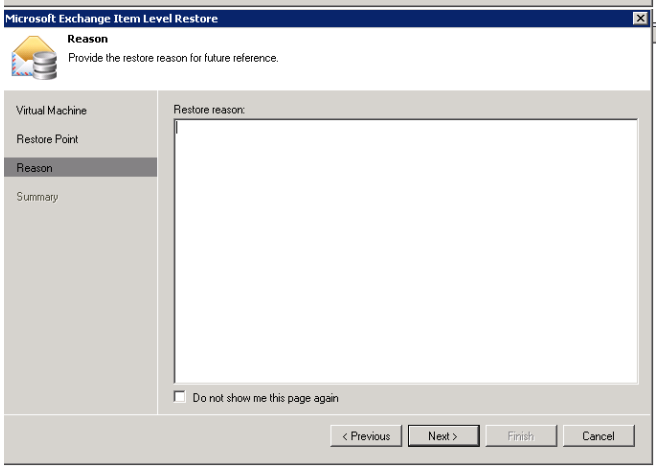
12	Check the 'Restore Summary' and click on "Finish"

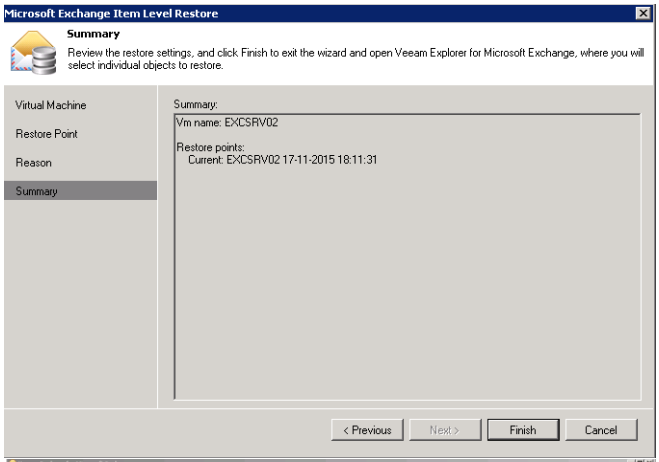
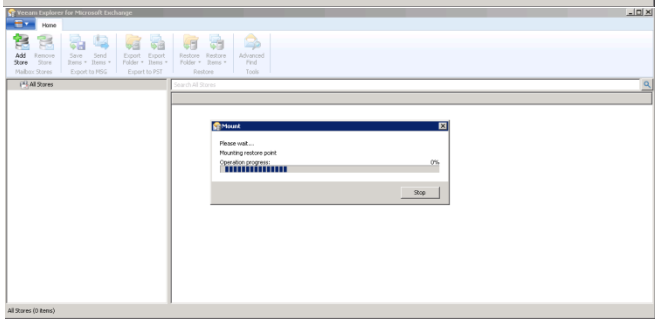
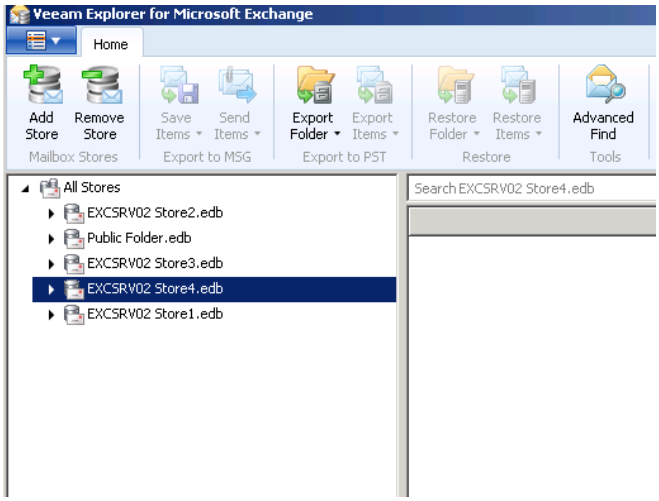


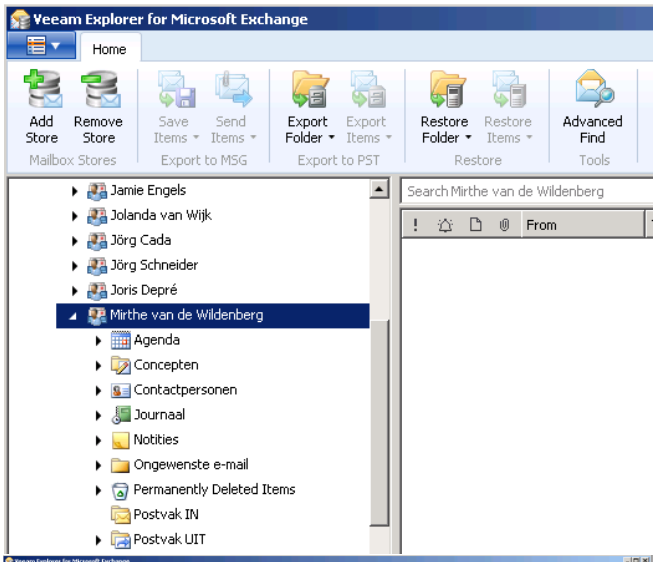
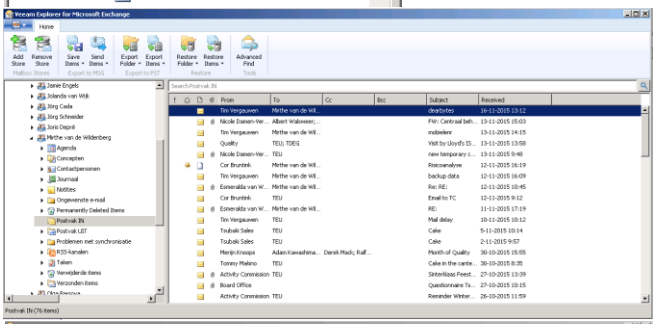
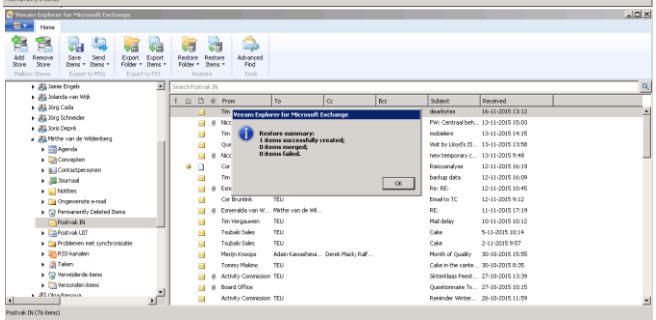
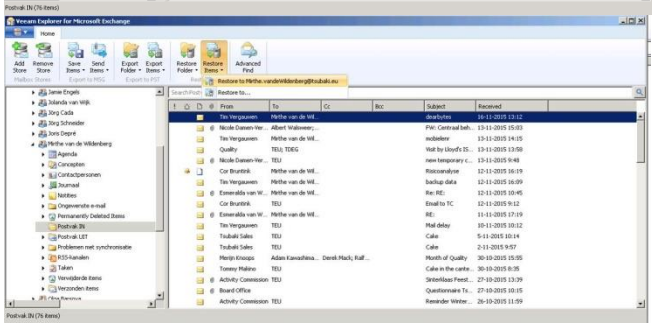
Appendix E - Microsoft Exchange 2010 restore procedure

Mailbox items Restore Procedure

EXCSRV02 (Veeam Backup & Replication)	
1	Start an RDP session to the "veeamsrv01" server and login
2	Open "Veeam Backup & Replication"
3	In the **Veeam Backup & Replication** menu, click on "Restore" and click on "VMware..." 
4	In the **Restore Options** menu, under *Restore from backup*, select "Application items" 
5	In the **Select Application** menu, select "Microsoft Exchange" to restore mailbox items (such as individual emails, appointments or contacts) 

6	In the **Virtual Machine** menu, select the Microsoft Exchange virtual machine to restore from Under *Exchange_DD*, select "EXCSRV02"	
7	In the **Restore Point** menu, select a restore point you want to restore from	
8	*Optional*: in the **Reason** menu, it is possible to specify a Restore reason and other additional information	

9	In the **Summary** menu, a summary of the restore is displayed Click on "Finish"	
10	The restore point will now be mounted:	
11	Under "All Stores", select a data store	

12	Select an email user account to restore mailbox items	
13	Select a folder and click on a mailbox item which needs to be restored	
14	When the **Restore summary** message is displayed, click "OK"	
15	Click on "Restore Items", and click on "Restore to <email address>" to restore the mailbox items to the corresponding user's email account ** Click on the "Restore to..." option if mailbox items from a particular user need to be restored to another user's email account*	

Appendix F - Motorola RFS6000 switch configuration

Appendix G - IT recovery startup sequence

The procedure below defines the order in which the IT systems and components need to function to be able to continue business functionality after a disaster has occurred.

Appendix H - Event log

Name: _____ **Title:** _____

Date: _____ / _____ / 20___ **Time:** _____

Description of disaster:

_____

_____

_____

Impact of disaster:

_____

_____

_____

Cause of disaster:

_____

_____

_____

Undertaken measures for recovery:

_____

_____

_____

_____

_____

_____

Bijlage 6 - Adviesrapport

Management Samenvatting

Gedurende dit project is onderzoek verricht naar de realisatie van een Disaster Recovery plan en hoe door de verantwoordelijken binnen Tsubakimoto ingegrepen dient te worden wanneer calamiteiten optreden binnen de ICT omgeving.

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

Middels het uitvoeren van een risicoanalyse zijn vervolgens de calamiteiten geïnventariseerd welke een fysieke impact hebben op de bedrijfskritische IT systemen, componenten en data. Om de kans en impact uit te drukken in meetbare resultaten, is gebruik gemaakt van de kwantitatieve methode.

Nadat de risicoanalyse is afgerond, zijn de correctieve en preventieve maatregelen gedefinieerd om het risico op calamiteiten te verminderen en waar mogelijk te voorkomen. De belangrijkste correctieve en preventieve maatregelen die betrekking hebben op calamiteiten welke dataverlies en verlies van IT systemen/ componenten tot gevolg hebben, zijn als volgt:

- Dataverlies kan onder meer een gevolg zijn van een virus aanval, onopzettelijke handelingen verricht door personeel of hardware falen. Om het risico op dataverlies te voorkomen, dienen dagelijks regelmatiger back-ups uitgevoerd te worden.
- Uitval van IT systemen en componenten kan te wijden zijn aan een brand, diefstal van IT apparatuur of hardware falen. In dit geval kan het (bij voorbaat) aanschaffen van vervangende IT apparatuur het risico op systeemverlies voorkomen.
- Door de IT apparatuur en componenten (zoals bekabeling) regelmatig te onderhouden en te controleren, kan potentiële schade/ defecten tijdig worden gesignaleerd en hersteld. Hierdoor wordt onder meer het risico op stroomuitval en systeemuitval geminimaliseerd.
- Verouderde (afgeschreven) IT apparatuur in gebruik dient vervangen te worden wat het risico op systeemuitval (hardware falen) verminderd.

Binnen Tsubakimoto zijn zogenaamde herstelteams, bestaande uit stafpersoneel, samengesteld die bepaalde handelingen uitvoeren in het geval van calamiteiten; wanneer calamiteiten zich voordoen, dient eerst ernst van de situatie te worden ingeschat. Wanneer het Disaster Recovery plan in werking is getreden, dient de impact (en eventuele schade) aan de IT systemen en componenten te worden vastgesteld. Daarnaast dienen klanten, personeel en leveranciers in het geval 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 (en dus de bedrijfscontinuïteit) te herstellen, moeten de herstelprocedures -- weke zijn 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.

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

- Voer een penetratietest uit om kwetsbaarheden in de beveiliging van IT systemen te detecteren. Kwetsbaarheden kunnen door hackers worden misbruikt, met als doel zoveel mogelijk schade te veroorzaken (bijv. het stelen van bedrijfsgegevens).

- Implementeer een redundante (failover) internetverbinding. In het geval de netwerk connectiviteit uitvalt, neemt de secundaire verbinding het over waardoor verlies van netwerk connectiviteit wordt voorkomen.

- Richt een alternatieve werklocatie in, om te voorkomen dat de bedrijfsvoering voor een lange periode niet functioneert. Hierin zijn drie varianten te onderscheiden, te weten: een 'Hot Site', een 'Warm Site' en een 'Cold Site'.

- 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.

- Het is aan te bevelen een tweede (redundante) core-switch in het netwerk te implementeren. In het geval een switch uitvalt, zal de secundaire switch de functionaliteit overnemen en wordt uitval van (netwerk)connectiviteit voorkomen.

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

- Het is aan te raden om een zogenaamde 'roll-back' test uit te voeren. Dit houdt in dat een calamiteit wordt gesimuleerd, waarin wordt getest hoe lang het duurt om te herstellen van calamiteiten, en of de omschreven herstelprocedures in het Disaster Recovery plan effectief zijn in de praktijk.

- Het is aan te raden om zowel het Disaster Recovery plan als de risicoanalyse uit te breiden en regelmatig te herzien. Hierbij is het belangrijk elk relevant risico op calamiteiten op te nemen in de risicoanalyse, wat uiteindelijk bijdraagt aan een effectiever Disaster Recovery plan. Wijzigingen in bijv. de bedrijfsvoering, of het introduceren van nieuwe apparatuur in de faciliteit dienen direct te worden aangepast in het Disaster Recovery plan.

- Onderzoek hoe er alsnog een passende oplossing gerealiseerd kan worden wat betreft het herstellen van configuratie van de SAN opslag omgeving.

1. Inleiding

Dit document omschrijft het adviesrapport voor het afstudeerproject "Disaster Recovery planning", welke is uitgevoerd binnen Tsubakimoto Europe B.V. te Dordrecht. Het voornaamste doel van dit adviesrapport is om middels aanbevelingen een advies te geven m.b.t. de preventieve maatregelen op lange termijn (wat betreft ICT gerelateerde calamiteiten) en het onderhouden van het Disaster Recovery plan.

1.1 Projectomschrijving

Dit afstudeerproject is tot stand gekomen in opdracht van Tsubakimoto Europe B.V. (hierna te noemen Tsubakimoto). Omdat Tsubakimoto niet beschikt over een Disaster Recovery plan, is het voor hen onduidelijk welke mogelijke calamiteiten zich kunnen voordoen binnen de ICT omgeving en hoe de verantwoordelijken hierbij moeten ingrijpen. Gezien de beperkte capaciteit binnen Tsubakimoto, is de hulp van de afstudeerder ingeschakeld om een onderzoek uit te voeren op het gebied van het realiseren van een inzetbaar Disaster Recovery plan.

Gedurende dit project is onder meer onderzoek verricht naar de realisatie van een Disaster Recovery plan en hoe door de verantwoordelijken binnen Tsubakimoto ingegrepen dient te worden wanneer calamiteiten optreden binnen de ICT omgeving.

1.2 Leeswijzer

Hoofdstuk twee omschrijft het verloop van de kritische bedrijfsprocessen binnen Tsubakimoto. Alvorens de mogelijke calamiteiten kunnen worden geïnventariseerd, dienen de kritische bedrijfsprocessen (waarmee de bedrijfskritische systemen gemoeid zijn) in kaart te worden gebracht.

In hoofdstuk drie is de IT apparatuur omschreven die de kritische bedrijfsprocessen ondersteunen. Daarnaast is er ook een tabel opgenomen waarin de relatie tussen de IT apparatuur en primaire bedrijfsprocessen schematisch wordt weergegeven.

Hoofdstuk vier omschrijft de risicoanalyse, waarin onder meer is beschreven welke calamiteiten zich kunnen voordoen binnen de ICT omgeving van Tsubakimoto. Daarnaast geeft dit hoofdstuk ook meer duidelijkheid over de gekozen methode wat betreft de beoordeling van de risico's op calamiteiten en wat de impact is hiervan op de primaire bedrijfsprocessen.

In hoofdstuk vijf wordt het Disaster Recovery plan (hierna te noemen: DRP) omschreven waarin onder meer is gedefinieerd welke maatregelen genomen moeten worden door de verantwoordelijken binnen Tsubakimoto, om spoedig te kunnen herstellen in het geval van calamiteiten.

Tot slot omschrijft hoofdstuk zes de conclusie en aanbevelingen, waarin onder meer de preventieve maatregelen zijn omschreven om calamiteiten te voorkomen op lange termijn.

Dit adviesrapport bevat het Disaster Recovery plan, welke apart is bijgesloten bij dit document.

2. 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 de haar klanten (met als mogelijk gevolg klanten en inkomsten te verliezen).

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).

Bovenstaande kritische bedrijfsprocessen hangen als volgt met elkaar samen: 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 magazijnbon, en worden de goederen geleverd aan de klant. De klant ontvangt hiervan een factuur (E. van Wensveen, persoonlijke mededeling, 27 november 2015).

2.1 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).

2.2 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).

2.3 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).

2.4 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).

2.5 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).

2.6 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).

2.7 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).

2.8 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).

2.9 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).

2.10 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[8]. De back-up van de virtuele servers wordt uitgevoerd door Veeam[9]. 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 backup-log. De back-ups worden vervolgens dagelijks gerepliceerd naar het (externe) datacenter (Tsubakimoto Europe B.V., 2014).

[8] 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/).
[9] 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).

2.11 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).

2.12 Procestabel

Tabel 1 weergeeft een overzicht van de IT systemen en componenten die de kritische bedrijfsprocessen ondersteunen. De specifieke services die worden geraadpleegd door een kritisch bedrijfsproces, zijn onder elk IT systeem/ component kort omschreven.

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			X	X		X	X	X	X	X	X

(magazijn bonnen).											
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 1 - Relatie IT systemen met kritische bedrijfsprocessen

3. Systeem inventarisatie

In dit hoofdstuk worden de IT systemen en componenten omschreven die de kritische bedrijfsprocessen ondersteunen. Hierbij gaat het om de volgende typen apparatuur: servers, switches, de router en de firewall. De "VM" (Virtuele Machine[10]) kolom in tabel 2 benadrukt of de server virtueel is geïmplementeerd. De gedetailleerde systeem inventarisatie is terug te vinden in het Disaster Recovery plan (appendix).

3.1 Systeem inventarisatie

3.1.1 Servers

Naam	Omschrijving	VM
ARSRV01	*Eagle presence registratie*	X
Barracuda Message Archiver 350	*E-mail archivering*	
Barracuda Spam Firewall 300	*Spam filter*	
CRMSRV02	*Unit4 CRM*	X
CTXSRV06	*Applicatie virtualisatie*	
CTXSRV07	*Powerfuse 2012*	X
	Citrix XenApp 6.5 Advanced Edition	
DATASRV03	*File server*	
	Limis planningssoftware	
	Tweede domain controller	
DBSRV01	*Agresso Wholesale back-up*	
DBSRV02	*Failover Agresso Wholesale*	X
DMNSRV02	*Domain controller*	X

[10] Een virtuele machine (VM) is een voorbeeld van een besturingssysteem in een geïsoleerde scheidingswand in een computersysteem. Hierdoor kunnen verschillende besturingssystemen tegelijkertijd draaien in dezelfde computer (Bron: http://www.pcmag.com/encyclopedia/term / 53927/virtual-machine).

	Domein gerelateerde taken uitvoeren	
	Safeword Token database	
	Citrix license server	
	Print server	
ELOSRV01	*ELO digitaal archief*	X
EMCDD01	*Back-up (en replicatie van back-ups naar externe locatie)*	
EXCSRV02	*Microsoft exchange 2010*	X
EXCSRV03	*Microsoft Exchange 2010*	X
FRONTENDSRV01	*Connectiviteit mobiele apparatuur*	X
LH-SAN01	*SAN opslag*	
LH-SAN02	*SAN opslag*	
LH-SAN03	*SAN opslag*	
LH-SAN04	*SAN opslag*	
PORTALSRV01	*DMZ*	X
	Citrix XenApp portal	
RFSRV01	*RF systeem*	X
SONICSRV01	*EDI Live omgeving*	X
SONICSRV02	*EDI Test omgeving*	X
	TopDesk	
TLSSRV02	*McAfee Epolicy Orchestrator 5.1*	X
	WSUS	
	Veeam One monitor	
VEEAMSRV01	*Veeam 8.0*	X
VPNSRV01	*Routering en Remote Access*	X
	Safeword	
VSPHERE01	*Server virtualisatie platform*	X
VMWSRV01	*VMware server*	
VMWSRV02	*Failover VMWSRV01*	
WEBSRV03	*DMZ*	X
	Unit4 WebSolutions	

Tabel 2 - Inventarisatie servers

3.1.2 Switches

Naam	**Omschrijving**
HP ProCurve 2920-24G-PoE	*Accesspoints van Aerohive WiFi zijn verbonden met deze switch*
HP ProCurve 4208VL	*De 'core switch' van het netwerk*
HP ProCurve E3500YL-24G-PoE (1)	*Onderdeel van de VMware omgeving*
	Onderdeel van de Failover omgeving
	Onderdeel van het iSCSI netwerk
HP ProCurve E3500YL-24G-PoE (2)	*Onderdeel van de VMware omgeving*
	Onderdeel van de Failover omgeving
	Onderdeel van het iSCSI netwerk
HP ProCurve 2610-12/24 PWR	*Onderdeel van de RF omgeving*
Motorola RFS6000 (Primary)	*Controller voor WiFi Accesspoints RF*
Motorola RFS6000 (Secondary)	*Failover switch*

Tabel 3 - Inventarisatie switches

3.1.3 Router

Naam	Omschrijving
Cisco Router C8536	*T.b.v. de internetverbinding*

Tabel 4 - Inventarisatie router

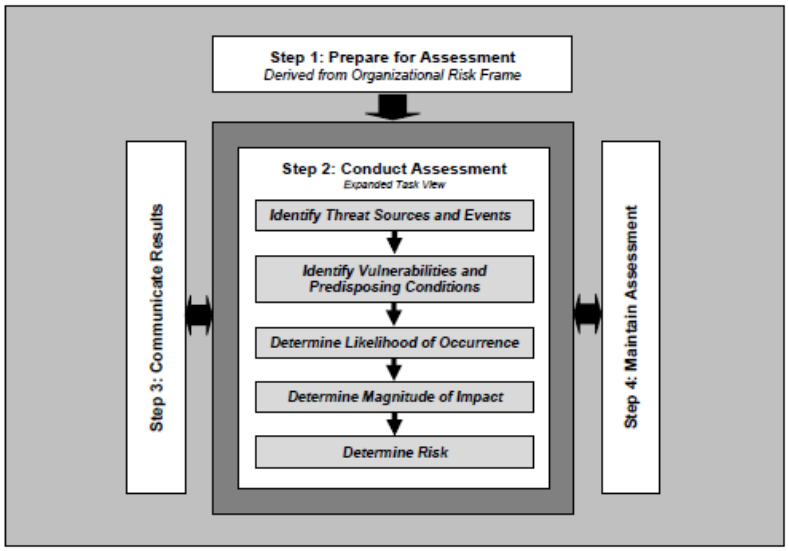
3.1.4 Firewall

Naam	Omschrijving
Juniper Firewall SSG140	*Gateway*
	VPN verbinding TUK (Tsubaki UK)
	VPN verbinding TDEG (Tsubaki Deutschland)

Tabel 5 - Inventarisatie firewall

4. 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). Deze standaard is gericht op de uitvoering van een risicobeoordeling op het gebied van de ICT. Met betrekking tot dit project zijn “Step 1: Prepare for Assessment”, “Step 2: Conduct Assessment” en “Step 3: Communicate results” uitgevoerd. Figuur 1 illustreert deze aanpak:



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

4.1 Risicocategorieën

Om de calamiteiten overzichtelijk te inventariseren, zijn in overleg met de opdrachtgever vier verschillende categorieën gedefinieerd, te weten: 'Natural & Environmental', 'Criminal', 'Personnel' en 'Technological'.

4.1.1 Natural & Environmental

Onder deze categorie vallen calamiteiten zoals brand en waterschade. Deze calamiteiten hebben mogelijk fysieke gevolgen voor de IT systemen/ componenten en dus ook op de continuïteit van de kritische bedrijfsprocessen.

4.1.2 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 in het ergste geval 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.

4.1.3 Personnel

Onder deze categorie vallen calamiteiten die veroorzaakt kunnen worden door onopzettelijk toedoen van 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.

4.1.4 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, systeem uitval en verlies van netwerk connectiviteit.

4.2 Methode

4.2.1 Kwalitatief

Een kwalitatieve beoordeling maakt gebruik van woorden of relatieve waarden om risico, kosten en impact uit te drukken (Snedaker, 2014).Het bereik van een kwalitatieve risicobeoordeling is echter relatief klein in de meeste gevallen, wat het moeilijker maakt om de prioriteiten of vergelijkingen binnen de set van gerapporteerde risico's te definiëren. De herhaalbaarheid en reproduceerbaarheid van kwalitatieve risicobeoordelingen worden verhoogd wanneer de geëvalueerde waarden (per niveau) worden ondersteunt door zinvolle omschrijvingen (bijv. deze waarde is "hoog" wegens de volgende redenen...) en wanneer tabellen worden gebruikt om kwalitatieve waarden te combineren (NIST, 2012).

4.2.2 Kwantitatief

Een kwantitatieve beoordeling maakt gebruik van metingen en getallen. Ze zijn specifiek en meetbaar (Snedaker, 2014). De nauwkeurigheid van kwantificering wordt echter verminderd wanneer persoonlijke opvattingen zijn gemoeid met de kwantitatieve beoordeling, of wanneer m.b.t. de vaststelling van de waarden een mate van onzekerheid gepaard gaat. Een kwantitatieve beoordeling biedt echter ook het voordeel dat de resultaten exact, herhaalbaar en reproduceerbaar zijn vast te stellen (NIST, 2012).

4.2.3 Semikwantitatief

Een semikwantitatieve beoordeling biedt zowel de voordelen van de kwantitatieve methode als de voordelen van de kwalitatieve methode en maakt gebruik van een risicobeoordeling welke gebruik maakt van schalen (bijv. 1-7, 8-14 en 15-25) welke eenvoudig te zijn vertalen in kwalitatieve termen

(bijv. een score van "20" kan worden geïnterpreteerd als "hoog"). Net als met de niet-numerieke categorieën die worden toegepast in de kwalitatieve beoordeling, dient elke schaal te worden verduidelijkt met een zinvolle omschrijving (NIST, 2012).

Omdat de opdrachtgever de behoefte heeft aan resultaten die middels berekeningen aantoonbaar kunnen worden onderbouwd, is met betrekking tot dit project in overleg besloten de kwantitatieve methode toe te passen.

4.3 Inventarisatie calamiteiten

In tabel 6 zijn de calamiteiten geïnventariseerd welke zich mogelijk kunnen voordoen binnen de ICT omgeving van Tsubakimoto. Hieronder vallen calamiteiten welke hun oorzaak vinden in de ICT omgeving (zoals hardware falen), en calamiteiten die gevolgen hebben voor de ICT omgeving (zoals een brand in de server ruimte).

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 offsite location.*	• There is currently no replacement IT equipment available (regarding a backup server).

Tabel 6 - Dreigingsanalyse

4.4 Effectenbeoordeling

In dit hoofdstuk is een schatting gemaakt van de kans en impact wanneer calamiteiten zich voordoen (tabel 7). Hierbij is de kans ('probability') gebaseerd op jaarbasis, en de impact gebaseerd op verloren manuren en hardware kosten. De risicofactor (Risk) wordt berekend met de volgende formule: Risk = Probability x Impact.

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 offsite location.*	0,0001	€ 6.000,00	€ 0,60

Tabel 7 - Effectenbeoordeling

5. 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.

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.

Communicatie
Wanneer calamiteiten optreden binnen de organisatie, moet er ook een omschrijving zijn waarin staat 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 herstel procedures) kan worden opgenomen in de bijlage van het DRP (Snedaker, 2014).

5.1 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. 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 (ElectricienNu, 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.

5.2 Herstelteams: rollen en verantwoordelijkheden

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.

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).

5.3.1 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).

5.3.2 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 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 is 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.

5.2.3 IT recovery team

Het IT recovery team komt nauw overeen met het damage assessment team, maar het IT recovery team heeft echter toch 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 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). 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.

5.2.4 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.

6. Conclusies en aanbevelingen

In dit hoofdstuk zijn 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 op lange termijn en hoe het Disaster Recovery plan opgevolgd dient te worden.

6.1 Conclusie

Gedurende dit project is onderzoek verricht naar de realisatie van een Disaster Recovery plan en hoe door de verantwoordelijken binnen Tsubakimoto ingegrepen dient te worden wanneer calamiteiten optreden binnen de ICT omgeving.

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

Voordat is gestart aan de realisatie van het Disaster Recovery plan, 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 de bedrijfskritische IT systemen en componenten in kaart gebracht die de kritische bedrijfsprocessen ondersteunen. Deze apparatuur omvat zowel de 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 bedrijfskritische IT systemen, componenten en data. Om middels meetbare resultaten aan te tonen wat de kans (op jaarbasis) en impact (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 de correctieve en preventieve maatregelen gedefinieerd om het risico op calamiteiten te verminderen en waar mogelijk te voorkomen. De belangrijkste correctieve en preventieve maatregelen die betrekking hebben op calamiteiten welke dataverlies en verlies van IT systemen/ componenten tot gevolg hebben, zijn als volgt:

- Dataverlies kan onder meer een gevolg zijn van een virus aanval, onopzettelijke handelingen verricht door personeel of hardware falen. Om het risico op dataverlies te voorkomen, dienen dagelijks regelmatiger back-ups uitgevoerd te worden.
- Uitval van IT systemen en componenten kan te wijden zijn aan een brand, diefstal van IT apparatuur of hardware falen. In dit geval kan het (bij voorbaat) aanschaffen van vervangende IT apparatuur het risico op systeemverlies voorkomen.
- Door de IT apparatuur en componenten (zoals bekabeling) regelmatig te onderhouden en te controleren, kan potentiële schade/ defecten tijdig worden gesignaleerd en hersteld. Hierdoor wordt onder meer het risico op stroomuitval en systeemuitval geminimaliseerd.
- Verouderde (afgeschreven) IT apparatuur in gebruik dient vervangen te worden wat het risico op systeemuitval (hardware falen) verminderd.

Binnen Tsubakimoto zijn zogenaamde herstelteams, bestaande uit stafpersoneel, samengesteld die bepaalde handelingen uitvoeren in het geval van calamiteiten. Deze handelswijze is als volgt; wanneer calamiteiten zich voordoen, dient eerst ernst van de situatie te worden ingeschat. Wanneer het Disaster Recovery plan in werking is getreden, dient de impact (en eventuele schade) aan de IT systemen en componenten te worden vastgesteld. Daarnaast dienen klanten, personeel en leveranciers in het geval 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 (en dus de bedrijfscontinuïteit) te herstellen, moeten de herstelprocedures -- weke zijn 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.

6.2 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. Kwetsbaarheden kunnen onder meer door hackers worden misbruikt om de beveiliging op de 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 redundante (failover) internetverbinding geeft een betere garantie voor de continuïteit van de bedrijfsvoering. In het geval de netwerk connectiviteit uitvalt, neemt de secundaire verbinding het 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. De bedrijfsvoering kan op deze wijze zo snel mogelijk (of al dan niet direct) worden hersteld in het geval van een desastreuze calamiteit (een brand 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 bandbreedte configuratie, kan de software en data worden ingeladen in de IT systemen);
    - 'Cold Site' (de hardware verplaatsen naar een alternatieve werkruimte met stroomvoorzieningen en netwerk connectiviteit).

- De router en de firewall die momenteel geïmplementeerd zijn binnen de netwerk infrastructuur 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 interne netwerk is niet redundant uitgevoerd. Indien deze switch uitvalt, ligt het interne netwerk stil en daarmee ook de communicatie tussen de server omgeving. Het is daarom aan te bevelen een tweede (redundante) core-switch in het netwerk te implementeren. In het geval een switch uitvalt, zal de secundaire switch de functionaliteit overnemen en wordt uitval van (netwerk)connectiviteit voorkomen.

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

- Nu er een Disaster Recovery plan 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 getest wordt hoe lang het duurt om te herstellen van calamiteiten, en of de omschreven herstelprocedures in het Disaster Recovery plan effectief zijn in de praktijk.

- Het is aan te raden om de risicoanalyse uit te breiden en regelmatig te herzien. Hierbij is het belangrijk elk relevant risico op calamiteiten op te nemen in de risicoanalyse, waardoor een zo compleet mogelijk beeld wordt gevormd van de potentiële calamiteiten die zich kunnen voordoen binnen Tsubakimoto. Daarnaast dienen wijzigingen in bijv. de bedrijfsvoering of IT omgeving direct te worden opgenomen in het Disaster Recovery plan. Dit zal uiteindelijk bijdragen aan een effectiever Disaster Recovery plan.

- Helaas is er gedurende het afstudeerproject geen oplossing gevonden om een herstelprocedure te omschrijven voor de SAN opslag omgeving. Bij deze wordt dan ook aanbevolen te onderzoeken hoe er alsnog een passende oplossing gerealiseerd kan worden wat betreft het herstellen van de configuratie van de SAN opslag omgeving.

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

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/

Kirvan, P. (2010). Risk assessments in disaster recovery planning. A free IT risk assessment template. Geraadpleegd op http://searchdisasterrecovery.techtarget.com/Risk-assessments-in-disaster-recovery-planning-A-free-IT-risk-assessment-template-and-guide

Kirvan, P. (2011). How to write disaster recovery plan and define disaster recovery strategies. Geraadpleegd op http://www.computerweekly.com/feature/How-to-write-a-disaster-recovery-plan-and-define-disaster-recovery-strategies

Kirvan, P. (2015). Risk analysis boosts disaster recovery planning process. Geraadpleegd op http://searchdisasterrecovery.techtarget.com/feature/Risk-analysis-boosts-disaster-recovery-planning-process

National Institute of Standards and Technology (NIST). (2012). *Guide for conducting risk assessments* [Special publication 800-30, Rev. 1]. Gedownload van http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.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 van http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Tsubakimoto Europe B.V. (2014). RE-10-4510-W-001-J - Back-up procedure.igx. Downloaded on 16-10-2015, from: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2014). RE-1-0060-W-001 - Control debtors.igx. Downloaded on 6-10-2015, from: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-3-1040-W-001 - Creating article record.igx. Downloaded on 6-10-2015, from: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-7-3003-W-001-K Manual Creditor payment.igx. Downloaded on 19-10-2015, from: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2013). RE-1-0050-W-001-K Margin control and invoicing.igx. Downloaded on 6-10-2015, from: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-5-2000-W-001-K Order collection, packaging and shipment.igx. Downloaded on 6-10-2015, from: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-3-1000-W-001-J Purchase order.igx. Downloaded on 6-10-2015, from: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2013). RE-5-2020-W-001-K Receipt goods and warehousing.igx. Downloaded on 6-10-2015, from: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2014). RE-10-4515-W-001-J - Restore procedure.igx. Downloaded on 16-10-2015, from: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-1-0020-W-001-J Sales order.igx. Downloaded on 6-10-2015, from: http://datasrv03/Tsubaki%20intranet/index.html

Tsubakimoto Europe B.V. (2015). RE-1-0010-W-001-J Sales quotation.igx. Downloaded on 6-10-2015, from: http://datasrv03/Tsubaki%20intranet/index.html