OWNER:	ISSUE DATE:	VERSION:
CUST-DEV2	13/12/2010	1.01

TAXATION AND CUSTOMS UNION DG
SPECIFICATION, DEVELOPMENT, MAINTENANCE AND SUPPORT OF CUSTOMS IT SYSTEMS AND APPLICATION

SUBJECT:

CUST-DEV2 DISASTER RECOVERY PLAN

CREATED UNDER SC02

CUST-DEV2

[REMOVED]

Security Notice: The information contained within this document has a confidentiality level classification of LIMITED. Unauthorized disclosure is prohibited. Failure to observe DG TAXUD decisions on security and the specification of the future Security Plan can result in disciplinary action, including dismissal.

Confidentially Classification: LIMITED

☒ Do not forward or copy data in part or full without explicit permission of Krist Teuwens

☒ Data access is limited to the **distribution access list specified below on this page**

☐ Use Strong authentication / EFS Encryption / Lock in a Drawer

☐ Log access in a register

☒ This version of the document is applicable after official acceptation by DG TAXUD. Until then the previous version, if existing, stays applicable

DISTRIBUTION ACCESS LIST

Name	Role	Access Type (Read Only/ Editor)
[REMOVED]	CUST-DEV2 Service Manager	Editor
[REMOVED]	CUST-DEV2 Service Manager backup and Programme manager	Read only
[REMOVED]	CUST-DEV2 Account Lead	Read only
[REMOVED]	Security Officer	Read only
[REMOVED]	System and Telecommunications Team	Read only
[REMOVED]	System and Telecommunications Team backup	Read only
[REMOVED]	CUST-DEV2 Riga Project Manager & Security Officer backup	Editor
[REMOVED]	Riga Project Manager backup	Read only
[REMOVED]	System and Network Administrator	Read only
[REMOVED]	System and Network Administrator backup	Read only
[REMOVED]	DG TAXUD R4	Read only
[REMOVED]	DG TAXUD R5	Read only
[REMOVED]	DG TAXUD LISO	Read only

[REMOVED]	DG TAXUD R5 APM	Read only
[REMOVED]	DG TAXUD R4	Read only
[REMOVED]	DG TAXUD Contract Management	Read only
[REMOVED]	DG TAXUD Contract Management	Read only

DOCUMENT HISTORY

Edi.	Rev.	Date	Description	Action (*)	Pages
00	00 01	26/07/2010	Creation of the Disaster Recovery Plan for the CUST-DEV2 SC02 Contract	I	All
00	00 02	29/07/2010	Internal review	I/R	All
00	01 00	9/08/2010	Submit for Review (SfR)	I/R	ALL
00	01 01	24/09/2010	Internal Review	I/R	ALL
01	00 00	29/09/2010	Submit for Acceptance (SfA)		
02	00 00	11/10/2010	Re-Submit for Acceptance (SfA) after correcting not accepted LISO comments with Reference #1,6,16 and 26	I/R	2, 11, 20-23, 32-40
03	00 00	14/10/2010	Re-Submit for Acceptance (SfA) after correcting not accepted LISO comments with Reference #1 – distribution list	I/R	2

(*) Action: I = Insert R = Replace

DOCUMENT CONTROL INFORMATION

Document Location

Softcopy of the document is located in ClearCase, [see 10.2.3]

Hard copy of the document is located in offline backup storage location, [see 10.2.2]

Document Scope

This document supports the recovery of the IT components for the operations delivered for DG TAXUD from Riga DC.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Reference and Applicable Documents

1.1 Reference Documents

When a document has been used to write another document or when reading a document can help the reader to understand more thoroughly a subject, this document is mentioned as a reference. This reference is explicitly mentioned here below using the reference Id.

The first point of reference is the TEMPO methodology.

Id	*Reference*	*Title*	*Version*
[RD1]	CUD2_SC02_CSP	Specific Contract 02 Contract Security Plan (CSP)	

Table **Error! No text of specified style in document.**-1: Reference documents

1.2 Applicable Documents

An applicable document is a document of which the content is binding for a contractor whether it is mentioned in this CQP or not.

Id	*Reference*	*Title*	*Version*
[AD5]	N/A	Open call for tenders **[REMOVED]** Provision of services for specification, development, maintenance and support of customs IT systems (CUST-DEV2)	Dated 21/03/09
[AD6]	N/A	Response to the open call for tenders **[REMOVED]**	Dated 18/05/09
[AD1]	N/A	Framework Contract TAXUD/2010/CC/100	N/A
[AD2]	N/A	Specific Contract 02 under the Framework Contract **[REMOVED]**	N/A
[AD3]	CUD_SC02_CQP	Specific Contract 02 Contract Quality Plan (CQP)	0.20-EN
[AD4]	TMP-POL-PAP	Tempo Password Policy	1.4

Table **Error! No text of specified style in document.**-2: Applicable documents

2 Terminology

2.1 Abbreviations and Acronyms

See Annex 19 for the full list of Acronyms and Abbreviations. These below are the relevant abbreviations for the DRP.

Abbreviations/ Acronym	Description
COTS	Commercial Off the Shelf Software
CQP	Contract Quality Plan
DG	Directorate General
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DRT	Disaster Recovery Team
FC	Framework Contract
FQP	Framework Quality Plan
HW	Hardware
IT	Information Technology
ITSD	Information Technology Support Department
OS	Operating System
QA	Quality Assurance
QC	Quality Control
QTM	Quoted Times and Means
RAID	Redundant Array of Independent Disks
RAS	Reliability, Availability and Serviceability.
REF	Reference
RTO	Recovery Time Objective
SC	Specific Contract
SE	Service
SW	Software
TAXUD	Taxation and Customs Union
T€S	Trans-European System
UPS	Uninterrupted Power Supply
VPN	Virtual Private Network
WP	Work Package

Table **Error! No text of specified style in document.**-3: Abbreviations and acronyms

2.2 Definitions

No definitions are provided.

3 IT DR Plan Introduction

3.1 Objectives

The primary objective of this Plan is to provide a plan of action to support the following recovery objectives:

- Risk reduction and prevention to help avert any interruption in computing systems, network or voice systems and services;
- Reduce confusion during any chaotic period by having a clearly defined course of action that will re-establish services as soon as possible;
- Identify critical functions with consideration of priority scheduling;
- Document any information (such as contact details, addresses, contacts for passwords) which might be needed in case of disaster;
- Provide the basis for the training of the Disaster Recovery Team (DRT);
- Identify the Disaster Recovery Resource for each item so that they can be called upon without delay when needed.

This plan aims to minimize:

- The number of decisions that must be made during and immediately after a major disruption;
- The organization's dependence on the participation of any specific person or group of people in the recovery process;
- The need to develop, test, and debug new procedures, programs, or systems during the recovery process;
- The adverse impact of any lost information and;
- Client's exposure resulting from a loss of IT services.

This plan outlines the documentation and planning necessary to implement operational capabilities. Additionally the possible cases of disaster are described along with the corresponding recovery actions performed by CUST-DEV2 contractor, the time needed for the recovery and the actors involved

3.2 Scope of the DRP

3.2.1 Cust-DEV2 is delivering 3 main types of services who can be impacted by a disaster.

- Development and maintenance of systems.

System related work will not be impacted by a disaster at the RIGA DC.
The source documents are hosted at the Hof DC and there will be working documents on the personal PC.
The SLA covered by the Hof DC are described in the table 4 hereunder.

Severity	Detail	SLA	Short Name
1	Major Outage/Application(s) unavailable/revenue impacting/no workaround/ whole site affected	80% in 4 hours	Major Outage
2	Urgent fits criteria for Priority 1 but workaround exists or significant impact to <25 people	80% in 1 Day	Critical
3	More urgent request, as it blocks a user from completing his tasks	80% in 3 Days	Urgent
4	Standard request, non business impacting	80% in 10 Days	Standard

Table **Error! No text of specified style in document.**-4: Hof DC SLA's

If the Hof DC is not available the work can continue on the personal computers.
When a personal computer experiences a disaster the source documents will still be available on the Hof DC. The internet connection when down can be restored in 2 to 4 hours.
Personal computers of CUST-DEV2 resources can be replaced between 3 and 8 hours.
For all these reasons Development and maintenance of systems will further not be in the scope of this DRP.

- Development and maintenance of applications.

Development and maintenance work of applications will be impacted in case of a disaster at the Riga DC.
Development, testing and training is done on the servers hosted at the Riga DC. These activities will be impacted in case a disaster occurs. In the worst case were all the servers are impacted by a disaster, e.g. an earthquake, explosion, etc., than CUST-DEV2 will not be able to deliver these activities until the servers are replaced.
In case the server farm is only partially impacted by the disaster than CUST-DEV2 will agree with DG TAXUD on the activities to reduce. The above will be in the scope of this DRP.
Development and testing is not executed in the Vilvoorde or Brussels location and therefore these activities would not be impacted in case of a disaster in these offices. Only training planed in these offices can be impacted by a disaster in these offices. In such a case CUSTDEV2 will contact DG TAXUD to reschedule the training on another date or/and at another location. For the above reason the Vilvoorde and the Brussels office are not in the scope of this DRP.

- 2e and 3e level support for incidents and corrective maintenance.

This activity will also be impacted in case of a disaster at the Riga DC. It will have the same impact as for the development and maintenance of the applications. This activity will be in the scope of this DRP.

3.2.2 Other tools or infrastructure that can be impacted by a disaster:

- CUST-DEV2 Corporate Assets:
  - *E-mail server of Accenture.*

  Most of the communication between DG TAXUD and CUST-DEV2 is done by e-mail.
  E-mail services going down will take between 2 and 4 hours to recover. When the recovery takes more than 4 hours the Service Continuity Management Lead will inform the Program Manager who will inform DG TAXUD. Communication which cannot wait for the recovery of the e-mail services can then be done by telephone. This service will further not be in the scope of this DRP.
  - Telephone:

  In case the telephone services are also not available then the program manager will indicate someone who will bring the message of the unavailability of the communication tools personally to DG TAXUD. This service will further not be in the scope of this DRP.
  - SharePoint

  SharePoint services going down will take between 2 and 4 hours to recover.

- Office infrastructure:

  Riga DC:

  - The server room is in the scope of this DRP
  - The Riga DC has two buildings available. If the offices used by CUST-DEV. would be unavailable because of a disaster, e.g. fire, than the resources can be re-located in the other building to continue working. If both buildings are impacted by the disaster, but the server room is still available, the resources can work from home. This will be in the scope of this DRP.

  Brussels and Vilvoorde location:

  - In case of a disaster at the Brussels location the resources located here can be moved to the Vilvoorde location.
  - In case of a disaster at the Vilvoorde location the resources located here can be moved to the Brussels location.

  The Brussels and Vilvoorde offices will be used only for project management related activities and for Systems related work. The resources can do this work also from home if these offices would be unavailable. These two locations will not be in the scope of this DRP.

3.2.3 Impacted assests per Work Package

Based on chapters 3.2.1, 3.2.2 and 3.2.3. Scope of the DRP are 4 categories of assests defined:

- PC used by the resources
- Corporate Assets : e-mail, phone, SharePoint
- Hof DC
- Riga DC

Per categorie of assests is indicated which Work Package is impacted.

	Needed Assets			
Work Package	**PC**	**Corporate Assets**	**Hof DC**	**Riga DC**
WP.0 Project Management				
WP0.1 produce & Maintain the FQP	X	X		
WP.0.3 Produce and Maintain the CQP	X	X		
WP.0.4 Produce Proposals for Specific Contracts (SC) and Request for Actions (RFA)	X	X		
WP.0.5 Internal activities: Quality Assurance (QA), Quality Control (QC), Risk Management,(RM), Self-Assessment (SA), Internal Audit (IA), Team Organisation and Management	X	X	X	X
WP.0.6 Interaction and Coordination with the Commission	X	X		
WP.0.7 Reporting	X	X		
WP.0.8 Planning	X	X		
WP.0.9 Co-operate with the Commission during Quality, Process and Security Audits				
WP.0.10 Delivery of Artefacts	X	X		
WP.0.11 Manage Procurement of Necessary Products and Services	X	X		
WP.2 Take-Over				
WP.2.0 Define the Detailed Take-over Plan	X	X		
WP.2.1 Take-over of Activities	X	X		
WP.5 Hand-over				
WP.5.1 Define the Detailed Hand-over Plan	X	X		
WP.5.2 Hand-over of Documentation, Source Code, Infrastructure	X	X	X	X
WP.5.3 Training and Support	X	X		X
WP.6 Specifications				
WP.6.1 Feasibility Study	X		X	
WP.6.2 Business & System Modelling	X		X	
WP.6.3 Requirements	X		X	
WP.6.4 Functional Specifications	X		X	
WP.6.5 Design	X		X	
WP.6.6 System Scope Management	X		X	
WP.6.8 Evolutive Maintenance of the Specifications	X		X	

	Needed Assets			
Work Package	**PC**	**Corporate Assets**	**Hof DC**	**Riga DC**
WP.6.9 Corrective Maintenance of the Specifications	X		X	
WP.7 Build and Test				
WP.7.1 Develop and Document Programmes or Software Components	X		X	X
WP.7.2 Produce Supporting Manuals	X		X	
WP.7.3 Produce Test Specifications	X		X	
WP.7.4 Perform Tests	X		X	X
WP.7.5 Release Assembling and Packaging	X		X	X
WP.7.8 Evolutive Maintenance of the Build and Test Software and Documents	X		X	X
WP.7.9 Corrective Maintenance of the Build and Test Software and Documents	X		X	X
WP.8 Service Management				
WP.8.1 Service Desk	X		X	
WP.8.3 The Business Perspective: liaison with the NAs, the contractors and the Commission Services	X			
WP.8.4 Application Management	X		X	X
WP.8.5 Security Management	X	X	X	X
WP.8.6 ICT Infrastructure Management	X			X
WP.8.8 Support Outside Business Hours	X		X	X
WP.10 Deliverables And Services on Request In The Scope Of The Framework Contract	X			

Table **Error! No text of specified style in document.**-5: Impacted Assets per Work Package

3.3 Assumption

The IT DR Plan has been developed for use if the Riga DC site has been rendered inoperable or unavailable or if an interruption to some or all business applications continues for an unacceptable period, and assumes the following:

- There are no critical applications running on servers in Riga DC;
- While some staff members may be unavailable by the disruption or its aftermath, sufficient personnel will be available to accomplish these tasks;
- The steps and functions documented in this plan are not intended to restore 'Business-as-Usual', they are intended to provide functionality sufficient only to avert catastrophic loss to DG TAXUD.

The other locations, Vilvoorde and Brussels, are not in the scope of this DRP. These locations are not running any applications and support only connectivity to the RIGA DC. This connectivity is not critical. The location hosting the ClearCase application is a delivered service and availability is part of the service contract.

3.4 Disaster Model

The vital records, possible threats to which the project is exposed together with the impact assessment of such events happening are described in the following sections.

3.4.1 Vital records

The project materials to be safeguarded specifically are:

- This disaster recovery plan;
- Vendors Contracts and Agreements;
- Configuration Management System, including client deliverables and Internal deliverables;
- Applications code;
- Project specifications and development documentation;
- Installation scripts and/or Install Shield projects;
- Equipment Inventory;
- Standard Operating Procedures;
- Telephone and contact Directories;
- Login and Password information;
- COTS and their corresponding documentation, licences and keys;
- Service management records (tickets, e-mails, etc.);
- The insurance contracts.

Where these materials are stored, who is responsible for the safeguarding and who has access to these materials will be described in the Security Plan [RD1].

There is no relative value for these records. All of these can or will be of high importance after a disaster.

Hereunder is the hardware and software listed as they are know and installed on the date this DRP is submitted. The list of hardware and software is maintained on a monthly basis and communicated to DG TAXUD as annex of the Monthly Progress Report.

Hardware Item identification	Type (HW/ HW+OS / OS/SWL	Serial N°	Location	Agreement type (Acquisition / renting / leasing)	Qty	ABAC Record (Y/N)	Installation Status
SUN SPARC Enterprise M5000 Server	HW	BCF102700B BCF102700A BCF1027009	Riga DC, Brivibas Street	Acquisition	3		Installed
Sun Fire X4170 Server	HW	1030XF512E 1030XF512A	Riga DC, Brivibas Street	Acquisition	2		Installed
Sun Fire X2270 server	HW	1030XFF067	Riga DC, Brivibas Street	Acquisition	1		Installed
Storagetek SAN 2540 - rack ready controller tray	HW	1029BE78BA	Riga DC, Brivibas Street	Acquisition	1		Installed
Storagetek SAN 2540 - 600 Gb SAS HDD expansion	HW	001022E0RMWY 3SL0RMWY	Riga DC, Brivibas Street	Acquisition	1		Installed
Storagetek SAN 2540 - 1 TB Gb SATA HDD expansion	HW	9QJ6WVAX GTA060PBJNZ3UF 9QJ6X7LW GTF002PBJSM61F 9QJ6ZYRS	Riga DC, Brivibas Street	Acquisition	5		Installed
Storeage tek SL24 tape library	HW	1022BRZ00G	Riga DC, Brivibas Street	Acquisition	1		Installed
Cisco MDS 9124 SAN switch	HW	JAF1422BGFD	Riga DC, Brivibas Street	Acquisition	1		Installed
Catalyst switch 3750	HW	SFCZ142471WN	Riga DC, Brivibas Street	Acquisition	1		Installed
FC server connect cable 2M	HW	n/a	Riga DC, Brivibas Street	Acquisition	7		Installed
LTO Gen 4 pack of 20 Tapes	HW	n/a	Riga DC, Brivibas Street	Acquisition	2		Installed
Server Rack	HW	2343VLY-1029PM0355 2343VLY-1029PM0356 2343VLY-1029PM0357 2343VLY-1029PM0358	Riga DC, Brivibas Street	Acquisition	2		Installed

					Maintenance			
Licence Identifcication	**Maintenance Supplier**	**QTY**	**Contract #**	**Warranty Valid Until**	**Start**	**End**	**RFA(s) of purchase, waranty renewals, etc.**	**Location**
Symantec Veritas NetBackup server & 5 standard client starter pack	Distrilogie	1					SC02-RFA10	Accenture RDC Brivibas, 214 & 214b LV-1039 – Riga Latvia
VMWare vSphere 4 essentials plus bundle for 3 hosts	Distrilogie	1					SC02-RFA10	Accenture RDC Brivibas, 214 & 214b LV-1039 – Riga Latvia
RenderX XEP Server Test/QA/Development 4x Server Quad-Core License	RenderX	1					SC02-RFA10	Accenture RDC Brivibas, 214 & 214b LV-1039 – Riga Latvia
Redix Network Server Based AnyToAny XML Format converter Engine for Windows 2003 srv	Redix	1					SC02-RFA10	Accenture RDC Brivibas, 214 & 214b LV-1039 – Riga Latvia
REDIX AnyToAny XML Format Converter engine - CAL for Windows	Redix	2					SC02-RFA10	Accenture RDC Brivibas, 214 & 214b LV-1039 – Riga Latvia
Redix AnytoAny XML format Converter Engine for 4 CPU SUN 10 Unix Dev/Test System	Redix	3					SC02-RFA10	Accenture RDC Brivibas, 214 & 214b LV-1039 – Riga Latvia
Toad for Oracle Professional	Quest Software	1					SC02-RFA10	Accenture RDC Brivibas, 214 & 214b LV-1039 – Riga Latvia
Toad for Oracle Standard	Quest Software	20					SC02-RFA10	Accenture RDC Brivibas, 214 & 214b LV-1039 – Riga Latvia
Exceed for Windows	Open Text	2					SC02-RFA10	Accenture RDC Brivibas, 214 & 214b LV-1039 – Riga Latvia

3.4.2 Possible Threats

A disaster is an exceptional and unforeseeable event, either of natural or human origin, having highly critical and negative impacts on the analysed elements (IT infrastructure and services) and which is also uncontrollable and very difficult to measure and monitor.

The first step in a risk assessment is the identification of possible threats. The threats have been can be categorized in:

Natural Disaster

Any natural disaster (e.g. fire, earthquake, floods, snow, etc.) striking the CUST-DEV2 contractor's premises will unavoidably disrupt the services provided by the CUST-DEV2 contractor's team.

Equipment failure

Equipment failures may disrupt the development/maintenance/support activities. The following threats are considered under the Equipment failure category:

- Power Outage;
- Network (internal/external) equipment failure;
- Computing equipment (server, storage, and workstation) failure.
- Airco interruption

Human failure

The following threats are considered under the Human failure category:

- Personnel unavailability (illness, accident, death);
- Resignation;
- Human error.

Hostile attacks

Hostile attacks aimed at harming (the organisation or the project) may jeopardise the integrity of the project material. The following threats are considered under the Hostile attacks category:

- Malicious code such as viruses, worms or Trojan horses;
- Network attacks such as Intrusions or Denial of Service attacks.
- Physical attacks

3.4.3 Assessment of likelyhood

After having identified the possible threats, as listed in the previous section, an evaluation is done on the likelyhood of such a threat going to interrupt the services provided.

For doing so a classification done using the following scale :

Numerical Scale	Qualitative Scale	Definition
5	Almost	Certain the threat is expected to occur in most circumstances (more than one in 12 months)
3	Likely	The threat could ccur at some time (once in 2 to 5 years)
1	Rare	The threat may occur in exceptional circumstances (less than once in 5 years or more)

Table **Error! No text of specified style in document.**-6: Likelyhood scale

Using the scale as specified above the likelood of the threats identified could occur is documented in the next table.

Category	Threat	Likelyhood
Natural Disaster	Fire, earthquake, floods, etc.	Rare
Equipment Failure	Power outage	Rare
	Network component equipment failure	Likely
	Computing component equipment failure	Likely
Human Failure	Personnel unavailability; Resignation	Almost
Hostile Attacks	Malicious code	Likely
	Network attacks	Likely

Table **Error! No text of specified style in document.**-7: Threat likelyhood assessment

3.4.4 Impact Assessment

The impact of an identified threats on the project is expressed using a scale as definted in Table Error**! No text of specified style in document.**-8.

Numerical Scale	Qualitative Scale	Definition
5	High	Serious damage: event that can casue a long term disruption of important part(s) of the service
3	Medium	Significant damage: event that with substantial management can be endured
1	Low	Modorate damage: event that with appropriate process can be managed

Table **Error! No text of specified style in document.**-8: Impact Scale

The table hereunder explaines the impact defined per category of disaster.

Category	Threat	Impact
Natural Disaster	Fire, earthquake, floods, etc.	High
Equipment Failure	Power outage	Medium
	Network component equipment failure	Medium
	Computing component equipment failure	Medium
Human Failure	Personnel unavailability; Resignation	Low
Hostile Attacks	Malicious code	Medium
	Network attacks	Medium

Table **Error! No text of specified style in document.**-9: Threats Impact Assessment

3.4.5 Risk Calculation

Combining the scores for impact and likelyhood of the possible threat the risk is calculated using the following formula :

Risk = threat likelyhood * {(impact score)**1.45}

Using the above risk formula a risk is classified into the following categories:

- “high” is the risk score is above 21;
- “Significant” if the risk score is more than 11, but less than or equal to 21;
- “Moderate” if the risk score is less than or equal to 11, but more than 5;
- “Low” if the risk is less than or equal to 5.

The next table classifies the identified risks into the applicable categorie using the above risk formula.

Category	Threat	Risk
Natural Disaster	Fire, earthquake, floods, etc.	Moderate
Equipment Failure	Power outage	Low
	Network component equipment failure	Significant

Category	Threat	Risk
	Computing component equipment failure	Significant
Human Failure	Personnel unavailability; Resignation	Low
Hostile Attacks	Malicious code	Significant
	Network attacks	Significant

Table **Error! No text of specified style in document.**-10: Risk Classification of identified Threats

Based upon the above risk classification, the required risk management strategy can be put in place to either reduce the likelyhood of a disruption, shorten the period of disruption, or limit the impact of a disruption.

3.5 Activation of the plan

The activation of the IT Disaster Recovery Plan is governed by the Accenture Crisis Management process with command and control implemented to manage the response, decision making and any recovery or restoration activities. The Crisis Service Manager Lead will be advised on the requirement to activate the plan.

3.6 Field of application

This document is applicable for the duration of the the Framework Contract FC **[REMOVED]**.

4 Recovery Team

4.1 Purpose

The Recovery Teams will be activated for the following reasons:

- To evaluate events leading to the decision concerning the declaration of a disaster.
- To execute the IT DR Plan to exercise the option of having hardware shipped to Riga DC for installation locally.

4.2 Structure

The following organization chart provides a summary of the recovery organization for the Disaster Recovery Plan. The complete contact details of the Recovery organization is maintained in Disaster Recovery Resources

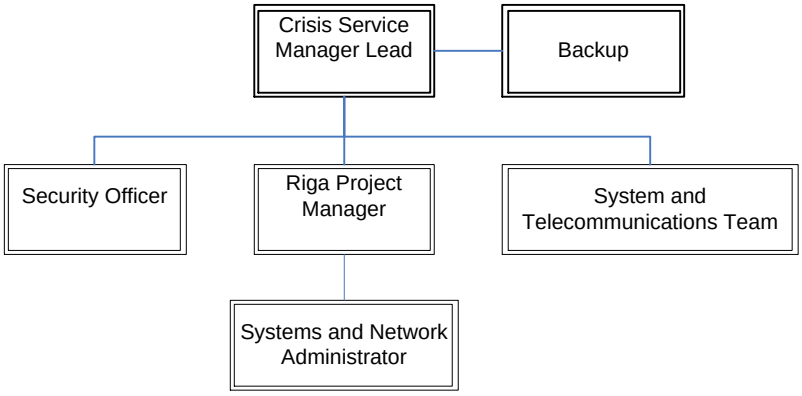

Figure 1: Organization for the Disaster Recovery Plan.

4.2.1 DRP Awareness

All the resources listed in Disaster Recovery Resources will be informed about the content of the DRP by receiving a copy of the present document and attending a presentation session organised within the month following its acceptance by DG TAXUD. The resources will receive a copy of the Disaster Recovery Plan at each update.

If Disaster Recovery Team Members or support infrastructure responsible persons change, their replacement will be informed of the DRP.

4.3 Disaster Recovery Team Roles and Responsibilities

The main purpose of the Disaster Recovery team is to coordinate all recovery activities and control the implementation of IT DR Plan. Some of the responsibilities are:

Role	Responsibilities
Service Continuity Management Lead	• During the recovery effort, the CUSTDEV2 contractor service manager will lead the project.

Role	Responsibilities
	This individual will: • Act as the focal point for mobilizing all resources necessary for the recovery process; • Liaise with Recovery Team • Coordinate all internal communications, • Coordinate all administrative requirements, • Be responsible for all on-going CUSTDEV2 contractor DR Plan maintenance, testing, and training.
Disaster Recovery Team (Network, Server, Messaging, desktop etc)	• Verify that the required technologies are restored • Identify and obtain any additional resources that are needed to restore critical business functions. • Monitor that the business application restorations are successful. • Prepare a schedule for staffing of technical personnel to support all business functions. • Check that all recovery tasks are appropriately executed. • Provide coordination and control of personnel relocated to the hot site. • Update the Crisis Management Team with the status of recovery activities.
System and Telecommunications Team	• Verify that phone lines are restored • Check that telecommunications lines are restored

Table **Error! No text of specified style in document.**-11: Reference documents

5 Communication Plan Overview

The diagram below (Figure-2) illustrates a high-level overview of how communication is managed during a business disruption.

All crisis communication with external stakeholders is via the Client Security Advisory Report (CSAR) which is supported by the crisis management process via Global Asset Protection team.

The operational communication to manage and support critical activities is performed by the Business Recovery team using their standard communication and escalation process defined for the operation.

IT recovery is one of the core business recovery elements which will be triggered to recover IT infrastructure so that business can recover their critical business functions during crisis.

This plan becomes effective when a major disruption occurs, and remains in effect until normal operations can be resumed.

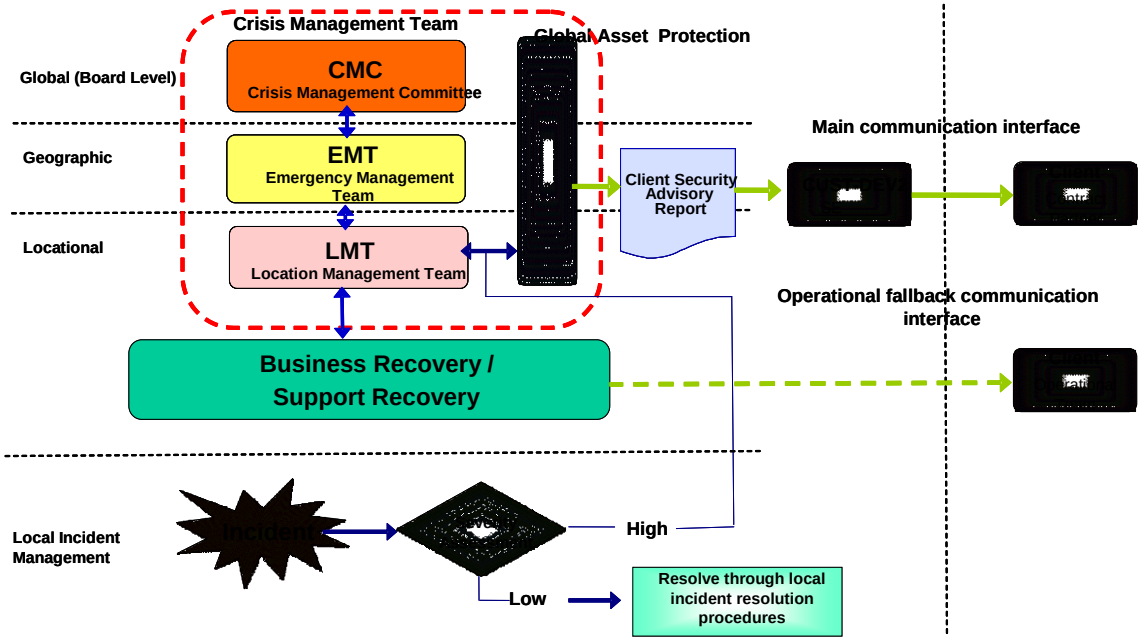

Figure 2 High level Communication Plan

The figure hereunder is describing who will communicate to who in case of a disaster.

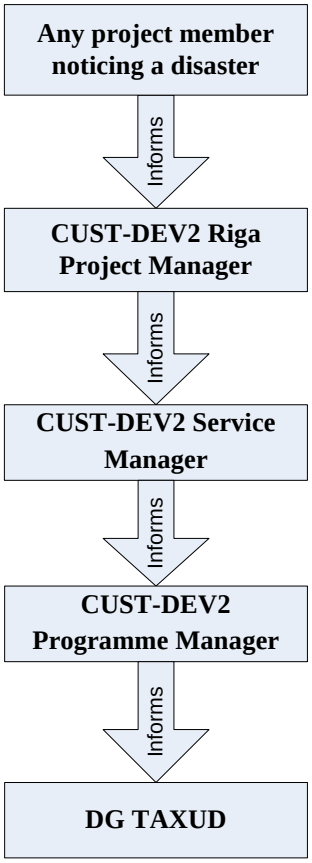

Figure 3 Communication detail.

6 Technology Infrastructure Overview and Disaster Recovery Plan

6.1 Infrastructure

This section provides the overview of existing IT infrastructure and its configurations. It also provides summary of Technology components, recovery strategy and how these components are configured, monitored, supported and maintained.

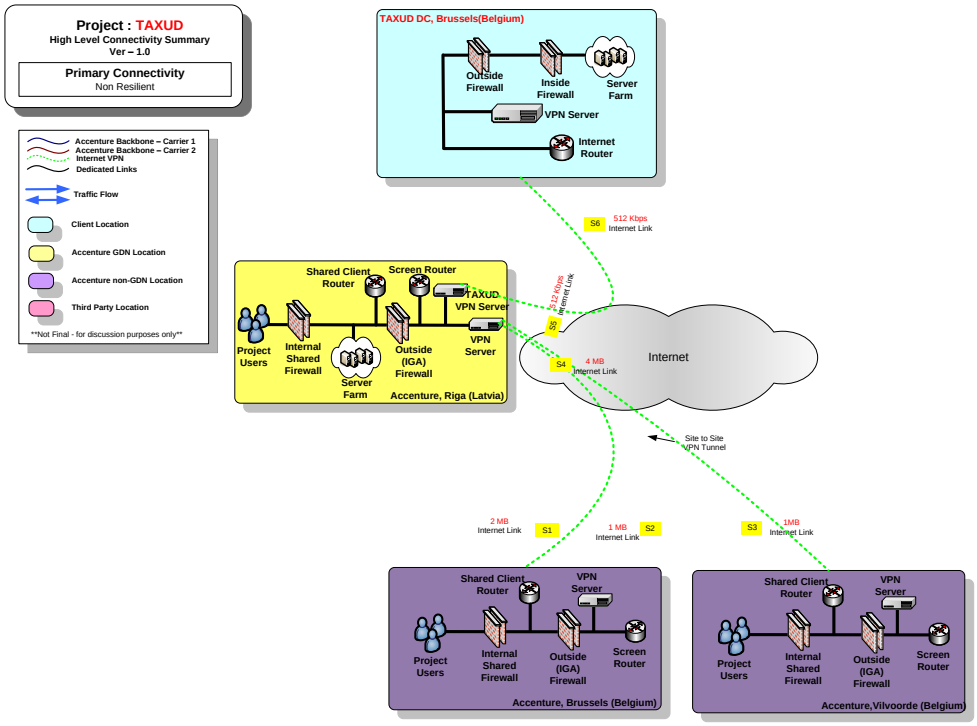

Figure 4 : Technology Infrastructure Overview

Riga DC has a Server Farm with infrastructure running development, QA, performance and production copy environment. Other locations – Brussels and client (DIGIT DC) are connecting to Riga infrastructure through VPN.

The figure hereunder give more detail on the Server Farm.

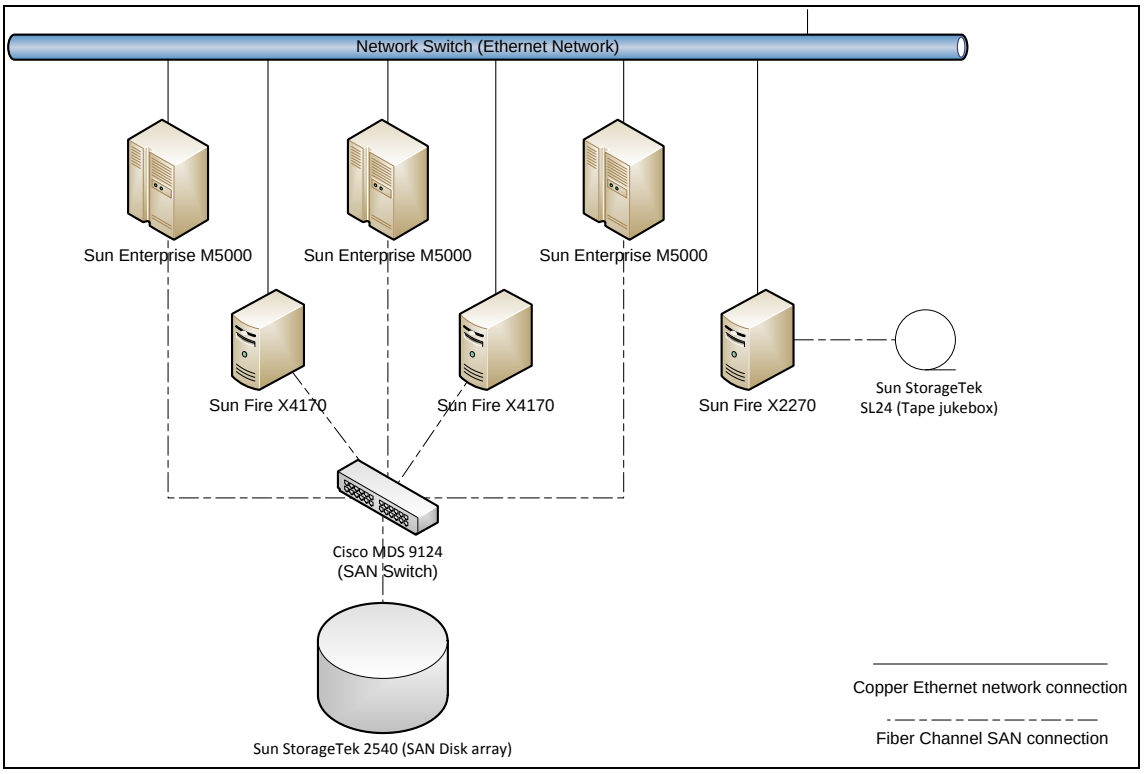

Figure 5 Development and Test Infrastructure Blueprint

The diagram below presents the high level application execution architecture setup.

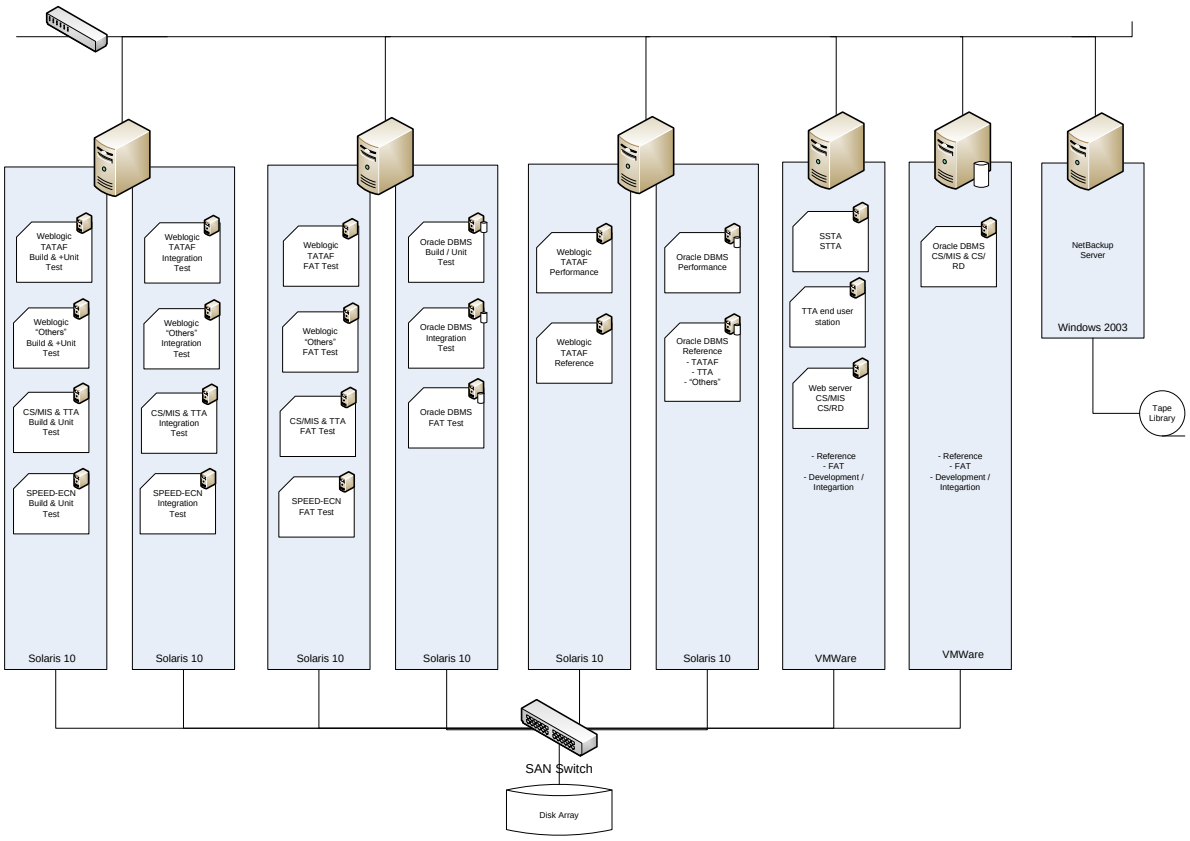

Figure 6 High level setup of the development and test server architecture

6.1.1 Development & Test Infrastructure

The ICT infrastructure presented in Annex F (Development and test environment) of the SC02 CQP [AD3] contains sufficient contingency measures to ensure a maximum availability in a development & test environment.

All proposed hardware contains the required RAS features to minimize the global unavailability of the hardware. It has to be noted that a disk failure as such cannot be considered to be a disaster as such a problem can be expected within reasonable time due to physical laws.

The most expedient strategy was the development of a short-term, high-impact plan that implemented sufficient procedures to handle a majority of the disaster situations that could occur.

6.1.2 Development Support Services Infrastructure

The development support services require the availability of the code & documentation central repository (Rational ClearCase) as well as the issue tracking application

(Rational ClearQuest), both part of the Accenture Delivery Tools family and being hosted at the Hof data centre, Germany. (See 10.2.3)

All records considered vital except hard copies (see 3.4.1) are maintained in ClearCase.

This data centre provides highly available services with estimated disaster recovery of all the services to a contingency site (another data centre within Accenture's global Delivery network) in 72 hours. Full daily and hourly incremental backup procedures are in place, with regular bi-annual tests of restore procedures.

The procedures related to installation of the Rational development support tools software, their configuration and the loading of the backup of their content databases are under configuration control within a separate ClearCase environment.

6.1.3 Physical Safety

The following Physical Safety measures are in place to protect the project infrastructure from natural disasters:

- All removable media units and backup media that are used on a daily basis are stored in a fire-resistant safety location to ensure that unauthorised persons cannot gain access to sensitive information while natural disaster recovery is also possible. This safety location is situated in another building in the street.
- All equipment is connected to an Uninterrupted Power Supply (UPS) network for the protection of the equipment, and the continuous service provision.

7 Recovery Approach

The chapter details first the preventative actions taken to reduce the risk of a potential threat. These preventative actions are of course considering the likelyhood of the threat happening as well as the impact of a possible threat on the services to be provided. The actions taken are then focussing on either reducing the likelyhood and/or the impact of the threat.

Besides the preventative actions, the chapter also then specifies the recovery actions to be taken in the event of such identified threat does happen. The target time for resuming service again after such incident, known as the Recovery Time objective (RTO), is the key unit of measure for such recovery actions. The RTO is of course aligned with the risk categorie assigned for the identified threat. The higher the risk categorie, the smaller the RTO will be.

7.1 Preventive Actions taken by CUST-DEV2

7.1.1 Security Officer

CUST-DEV2 contractor has nominated a **Security Officer** who is responsible for ensuring security of the CUST-DEV2 contractor's premises and access to relevant information. The objective is to protect both CUST-DEV2 contractor's internal assets, as well as DG TAXUD assets and to comply with external regulators and auditors. The Security Officer will organize security awareness sessions for the CUST-DEV2 project members. He controles if the security measures ae in place and if security risk mitigation is applied and respected. He controls also if the physical protection measures are up and running, e.g. fire alarm is working, fire extinguisher in place and operational, access control active. The Security Officers advice management of CUST-DEV2 contractor on all possible issues related to information security, whatever related to both DG TAXUD information security as well as to information security. The project appointed Security Officers reports to the CUST-DEV2 contractor's Programme Manager.

7.1.2 System Administrator

CUST-DEV2 contractor has nominated a **System Aministrator** who is responsible for ensuring security of the servers and installed applications. He will monitor the system process and acces on the servers. He assures that all security measures are applied and followed by the users for the servers and applications. The System Administrator advice management of CUST-DEV2 contractor on all possible issues related to the server security and the server operations. The project appointed System Administrator reports to the CUST-DEV2 contractor's Service Manager.

7.1.3 Security Risks Mitigation

The table that follows provides the measures to be taken by CUST-DEV2 contractor's team, to mitigate the project security risks introduced by the threats identified in the

previous section. It must be mentioned that mitigation measures may be taken either at the CUST-DEV2 contractor's corporate or project level.

Threat	Mitigation Measures
Natural Disasters	Physical safety infrastructure, basic protection is installed, e.g. fire protection. Backup procedure will secure all installed SW and the configuration. The Back-up procedure will be described in detail in the Securty Plan [AD1].
Power outage	Physical safety infrastructure, UPS will cover the period to perform a controlled power-off of the equipment.
Network equipment failure	Backup procedure will secure all installed SW and the configuration. The Back-up procedure will be described in detail in the Securty Plan [AD1].
Computing equipment failure	Backup procedure will secure all installed SW and the configuration. The Back-up procedure will be described in detail in the Securty Plan [AD1].
Personnel unavailability	Information Storage on a Central Repository. All documentation is stored in ClearCase hosted at the Hof DC.
Malicious code	Antivirus Policy: detail described in the Security Plan [AD1].
Network attacks	Electronic Access Control Procedure. Electronic Access Control Infrastructure. Access to the Network and Infrastructure is detailed in the Security Convention

Table **Error! No text of specified style in document.**-12: Security Risks & Mitigation Measures

7.1.4 Procedures

All access control (physical and electronic); backup, storage and archiving related policies and procedures are detailed in the security plan deliverable [RD1].

7.2 Recovery from Natural Disasters

A natural disaster can have an impact on the computer room, the development workstations or human resources.

7.2.1 Initial Response

The responses will take place separately or simultaneously.

Disaster Recovery Team Notification

- Any employee of CUST-DEV2 contractor could be the witness or the first to discover a disaster on one of the premises. After calling needed emergency services, as indicated in the premises emergency instructions, he/she must call the management of the affected premises who needs to notify the CUST-DEV2 Disaster Recovery Team of the disaster.
- The contact list in case of dissaster will be part of the welcome kit for resources starting on the CUST-DEV2 project.Depending upon the severity of the emergency the Service Continuity Management LeadDisaster Recovery Coordinator willshould be notified immediately. In most of the cases this will be only the case of a major disaster. For example a disk failure which is covered by the RAID 5 protection, or the unavailability of a resource for 2 days, is no major disaster and can be handled without the intervention of the Service continuity Management Lead. A complete server to replace is a major disaster and will need a notification of the Service Continuity Management Lead. The Coordinator maintains an emergency notification list and will ensure that all required personnel have it available. If the Coordinator cannot be reached other members of the Disaster Recovery team will be called until one of them is notified.
- The first member of the Disaster Recovery team to be notified is responsible to notify other critical members of the team and to initiate action. The Disaster Recovery team will call other specialists with current information on the disaster and instruction as appropriate.
- The Crisis Service Manager Lead will inform the program manager who will inform DG TAXUD: at least the contract management responsible and the application project manager for the applications impacted by the disaster.

Initial Disaster Management Procedures

- Once the Disaster Recovery team has been notified, they will proceed to make an immediate assessment of the situation and to initiate appropriate actions.
- If the Disaster Recovery Coordinator has not yet been contacted, an alternate shall be selected by the Disaster Recovery team and will assume full responsibilities of the Disaster Recovery Coordinator, until he or she has arrived and been fully briefed. The Disaster Recovery Coordinator or acting Coordinator will proceed to implement the contingency plans.
- Make an assessment of the situation directly at the scene if possible, or if not, indirectly based on reported information from the notification sources.
- Based on the Disaster Recovery team assessment of the situation, determine the severity of the problem and decide on the appropriate actions.
- If the The Crisis Service Manager Lead determines the emergency to be a major disaster, proceed to do the following:
    - Notify the appropriate emergency teams;

- Notify the Top Management;
- Determine viable contingency alternatives.

- If the Disaster Recovery team does not determine the emergency to be a major disaster, then the appropriate correction or recovery procedure will be implemented. In such a case, selected recovery teams may or may not be called upon to take action.
- The DG TAXUD representatives are kept informed of the decisions: at least the contract management responsible and the application project manager for the applications impacted by the disaster.

Notification of Necessary Disaster Teams

- In the event of a major disaster scenario, the CUST-DEV2 contractor's Management will be notified of the emergency by the Recovery team. The CUST-DEV2 contractor's Management will be kept appraised of the status of personnel, property, and the recovery effort.
- Determine if a Disaster Recovery Team should be activated and if the presence of additional support is required to support the recovery activities or contingency procedures.
- Notifications to CUST-DEV2 contractor's Management should cover what happened, the current status, the plan of action, and the location and phone numbers of the Recovery team. They should also be informed whether their presence is required and when.
- Notifications to the Disaster Recovery Team should cover what happened, the current status, the plan of action, and the location and phone numbers of the Recovery team.
- All Disaster Recovery team members will bring their personal copies of the Disaster Recovery Plan and other documentation for which they are responsible to the emergency coordination meeting. The Source documents are stored in the configuration management tool (ClearCase) which is hosted in separate data centre with full operation recovery SLA estimated to 72 hours. More information on the SLA's agreed with the Hof DC can be found in the CQP [AD3].

Disaster Recovery Team Coordination

- When all of the required Disaster Recovery team have been assembled at the location defined at the moment of the disaster notification (mostly the Disaster Recovery Coordinator office), the Disaster Recovery Coordinator will brief them on what has occurred and provide an overview of the Disaster Recovery team assessment of the status.
- It's up to the Disaster Recovery Coordinator to decide to wait or not for all the members of the Recovery Team.
- The teams should collectively discuss all of the basic aspects of the situation, and considerations of problems due to the processing schedule or anything else, before proceeding to carry out their individual team functions.

- Before any team leaves, the Disaster Recovery Coordinator will review with each team leader the actions that each team will be taking.
- The DG TAXUD representatives are kept informed of the decisions: at least the contract management responsible and the application project manager for the applications impacted by the disaster.

Contingency Operations Procedures

- The Disaster Recovery Team will assemble for briefing, discussion of any identified problems, and coordination of the recovery effort.
- If hardware has been destroyed, damaged, or negatively affected, the needed Teams will take the appropriate action to repair or replace the affected hardware by calling the concerned hardware provider who will intervene according to his support contract.
- If phone lines have been destroyed, damaged, or negatively affected, the needed Systems and Network Teams will take the appropriate action to repair or replace the affected lines by calling the concerned telecommunication provider. In the intervals, all the parties identified as CUST-DEV2 contractor's Service Requesters (DG TAXUD and/or its contractors) will be informed about the situation and provided with emergency mobile phone numbers to be able to reach CUST-DEV2 contractor.
- If telecommunications lines used for electronic mails have been destroyed, damaged, or negatively affected, the needed Telecommunications Teams will take the appropriate action to repair or replace the affected lines by calling the concerned telecommunication provider. In the intervals, all the parties identified as CUST-DEV2 Service Requesters (DG TAXUD and/or its contractors) will be informed about the situation and provided with emergency phone numbers to be able to reach CUST-DEV2.
- If facilities have been destroyed, damaged, or negatively affected, the Disaster Recovery team will liaise with CUST-DEV2 contractor's Management who will take the appropriate action to repair or replace the affected facilities. In the intervals, all the parties identified as CUST-DEV2 Service Requesters (DG TAXUD and/or its contractors) will be informed about the situation and provided with emergency mobile phone numbers to be able to reach CUST-DEV2.
- The Disaster Recovery team will coordinate the contingency operations until they can be returned to a normal, non-emergency state.

7.2.2 Restoring Original Operations

7.2.2.1 Hardware replacement

Depending on the component, vendor maintenance agreements may cover replacement or the order time can range from a few days to two months for hardware systems from the original hardware vendors. Used equipment vendors usually have hardware available for immediate shipping; in most cases delivery could be expected within six weeks. The Contracted vendor for equipment in the event of an emergency can also provide permanent replacement hardware.

7.2.2.2 Computer Room

A disaster in the computer room will cause damages on the H/W infrastructure and on the network/telecommunication facilities. The recovery steps are the following:

Recovery steps	Procedure	Duration (RTO)	Actors Involved
HW Procurement	Retrieve the characteristics of the machines by the H/W inventory maintained Procure required H/W	≈40 working days	System and Telecommunications Team, CUST-DEV2 Contractor's Alliance Team, Administrative Assistant, Service Manager
Set up of network	Retrieve the characteristics of the network components by the H/W inventory maintained (for the internal company infrastructure) Re-establishment of communication between company and network provider Network configuration (routers, servers, switches configuration) Re-establishment of telecommunications	≈30 working days for Re-establishment of communication between company and network provider ≈15 working days for Network configuration (routers, servers, switches configuration) ≈45 working days for Re-establishment of telecommunications (around 40 days are for the replacement of telephone centre)	System and Telecommunications Team, CUST-DEV2 Contractor's Alliance Team, Administrative Assistant, Service Manager
Full Recovery of system and applications software environment	Restoration (replacement) of a corrupt system The following procedure is applied for the replacement of a corrupt system: Install a minimum operating system from CD or tape. 1. Insert the most recent monthly backup tape and restore the system.	≈2 working days, assuming hardware is unaffected	CUST-DEV2 contractor's administrator team

Recovery steps	Procedure	Duration (RTO)	Actors Involved
	2. Insert the most recent weekly backup tape and restore. 3. Insert the most recent daily backup tape and restore.		
Set up a new CCN/CSI gateway	Contact with Taxation and Customs Union DG	≈50 working days	Taxation and Customs Union DG

Table **Error! No text of specified style in document.**-13: Recovery Steps for the catastrophe of the Computer Room

It should be mentioned that the steps (1), (2) and (4) indicated in Table Error**! No text of specified style in document.**-13 can be performed in parallel. In this sense the time needed for CUST-DEV2 contractor to be functional is reduced significantly.

7.2.2.3 Development Workstations

Recovery steps	Procedure	Duration (RTO)	Actors Involved
Workstation Procurement	Retrieve the characteristics of the machines by the H/W inventory maintained by the ITSD stored in the safety deposit box	≈10 working days	CUST-DEV2 contractor's Alliance Team, Administrative Assistant, Service Manager
Workstation configuration	Operating system installation, network configuration, antiviral software installation, necessary development environment/tools installation/configuration	≈half working day per workstation	CUST-DEV2 contractor's administrator team

Table **Error! No text of specified style in document.**-14: Recovery Steps for the catastrophe of the Development Workstations

7.3 Recovery from Equipment Failure

7.3.1 Power Outage Recovery

The UPS used provides electricity for maximum one hour, which should give enough time for a controled shut down of the servers and network equipment by the system administrators.

The RTO for such power outage is maximum 1 day.

7.3.2 Network Equipment Recovery

The network equipment is covered with the necessary HW maintence and support contracts enabling a RTO of maximum a few days.

7.3.3 Computing Equipment Recovery

Depending on the type of the computing equipment either server or workstation we follow the procedure described in sections 7.2.2 and above 7.2.2.3 regarding procurement and configuration.

Depending upon the size of the computing equipment damage the RTO will be in the range from either a few days or weeks.

7.4 Recovery from Personnel Unavailability

Personnel unavailability might be caused due to illness, accident, death, or resignation. For the first cause, CUST-DEV2 contractor maintains a central repository where applications software and documentation are available by authorised users.

For the case of resignation CUST-DEV2 contractor will organise internally on a continuous basis training sessions and meetings where cross fertilisation of knowledge is ensured. In addition, for each relevant person in the CUST-DEV2 contractor's team, a back-up person is assigned to take over the relevant person's responsibilities in case this is requested.

In case of the unavailability of a large group of resources, e.g. due to a epidemic, DG TAXUD will be contacted to agree on which services can be reduced or delayed.

7.5 Recovery from Hostile Attacks

7.5.1 Malicious Code

The antiviral policy of CUST-DEV2 contractor is made in a manner that this type of disaster has a very low probability. If such an event occurs the relevant CUST-DEV2 contractor's security officer will be informed and together define the appropriate steps on how to proceed with the cleanup procedure.

The RTO for such case is a few days at maximum.

7.5.2 Network Attacks

The security policy of CUST-DEV2 contractor's is made in a manner that this type of disaster has a low probability since a firewall presence and a restrict access to corporate routers exist.

In case of attack, CUST-DEV2 contractor's experienced network engineers investigate the penetration way and the security policy of the company is adjusted accordingly.

The RTO for such case is a few days at maximum.

7.6 Recovery of CUST-DEV2 Specifications documentation

All the CUST-DEV2 contractor's documentation produced so far is stored in the ClearCase, see 10.2.3.

7.7 Recovery of Applications within CUST-DEV2

All the CUST-DEV2 contractor's software purchased so far is stored in the ClearCase, see 10.2.3.

8 IT DR Plan Maintenance

8.1 Periodic Maintenance

IT DR Plan is maintained on an on-going basis and any changes must be reviewed and approved by the Service Continuity Management Lead.

The entire Plan and its Appendices should be reviewed on an annual basis to verify applicability.

8.2 Ongoing Maintenance

Revisions to this Plan must be considered anytime changes occur within the organization. Types of changes that could affect the Plan include:

- Infrastructure changes;
- Staff changes;
- Support service changes;
- Addition/deletion/changes of business requirements;
- Change requirements based on Test results.

The Service Continuity Management Lead has primary responsibility for ensuring that updates to the Plan and Appendices are completed in a timely manner.

9 IT DRP Plan Testing

9.1 Objectives

- To plan and schedule at least once a year a test of the DRP and maintain a calendar of the planning;
- To identify any weaknesses or oversights in the recovery plan by performing testing;
- To evaluate the test against its objectives to determine its effectiveness;
- To train personnel in executing the plan;
- To revise the recovery plan based on the results from the test.

9.2 Approach

Recovery plan validation is accomplished by testing various parts of the plan at different levels. Each test is carefully planned to ensure that everyone understands its objectives and agenda. It is then conducted by performing procedures from the plan as if a real disaster had occurred. Finally, the test is evaluated against its objectives to determine its effectiveness and to identify updates, which need to be made to the plan. The evaluation and and actions will be documented in the Test Report.

9.3 Plan the Test

9.4 If the recovery plan is properly tested, the risk of failure after an actual disruption is significantly reduced. For testing to be beneficial, it must be carefully planned including what should be tested, how it should be tested, and whom the test should involve. TConduct the Test

This step involves briefing the test team about the test and then executing it. As the test is conducted, documentation will be produced which will be evaluated after the test to determine the test's results. This will help to detect any oversights that may exist in the plan and it will verify that the recovery plan can be executed effectively. Testing the plan is also a good way to familiarize personnel with the recovery plan and the importance of maintaining it.

The following sections contains all aspects of the overall test program that must be filled out for each test is completed.

9.4.1 Define the test case

Possible test cases are :

- Riga office is not available
- One of the servers is not available
- One Resource is not available

Detail test plans can be found in chapter 9.5.

9.4.2 A test will be documente as follow

9.4.2.1 General Information

The following section contains an overview of relevant test information. This information is filled in by the individual responsible for the test.

Test Date:	
DRP Test Organized By:	
Service Manager:	
Test Conducted By:	
Area Tested:	
Test Approved By:	

9.4.2.2 Test Participants

This section contains information relating to the individuals who were present at the test.

Test Participants:	
1.	
2.	
3.	
4.	

9.4.2.3 Plans and Procedures Used

The following section contains all the plans and/or procedures utilized. Depending on the type of test there will be a requirement to use different processes.

Plans and Procedures Used:	
1.	
2.	
3.	
4.	

9.4.2.4 Assumptions

It is important that any assumptions made are clearly outlined prior to the test session. When reviewing the test results it is important to look at the assumptions as they provide further insight in to the test that was being conducted and any assumed conditions.

Assumptions:	
1.	
2.	
3.	
4.	

9.4.2.5 Scope

Depending on the test occurring, one or more business units and/or systems will be involved in conducting the test.

Business Unit	System	Comments

9.4.2.6 Required Roles and Responsibilities

The following section contains a list of the individuals who will be required to be involved in the test and their responsibilities. Each individual must be comfortable with their responsibilities. If individuals identify weaknesses or gaps in their process this will be highlighted in the notes and the appropriate assessment conducted.

Duties & Responsibilities:	
Individual	**Duties**

9.4.2.7 Entry and Exit Criteria

The following table is a template to be used for the entry and exit criteria that will be used in the testing plans. The entry and exit criteria may be expanded depending on the complexity of the system and the depth of testing that VENDOR wishes to conduct. It is essential that all entry and exit criteria are listed here so the Service Restoration Teams are provided with clear testing parameters.

Test Cycle	Entry	Exit

9.4.2.8 Dependencies and pre-test tasks

This section contains the dependencies and pre-test tasks that must be completed before training may begin. It is essential that all these tasks have been completed and signed off as failure to complete a task may negatively impact the overall business.

Task	Responsibility	Completed?

9.4.2.9 Tasks to set-up the environment

Task	Timing	Completed?

9.4.2.10 Execution of Disaster Recovery Process

Activity	Expected Results	Actual Results Observations	Owner	Success Yes/No	Comments

9.4.3 Post DR Test Tasks

The following section contains the post tasks that must be conducted after DR Test has been completed. This will include continued review of results and treating of risks.

Task	Timing	Completed?

Task	Timing	Completed?

9.5 Test Plans

The 4 Test Plans hereunder will be adjusted after each test run if necessary.

If the need is expressed by DG TAXUD or CUST-DEV2 other test cases will be defined.

9.5.1 Power outage at the RIGA DC

9.5.1.1 General Information

Test Date:	To be completed
DRP Test Organized By:	Riga project Manager
Service Manager:	**[REMOVED]**
Test Conducted By:	Riga project Manager
Area Tested:	Power outage at the RIGA DC
Test Approved By:	Service Manager

9.5.1.2 Test Participants

Test Participants:	
1. Riga Project Manager	**[REMOVED]**
2. Systems and Telecom Team	Rodions Sirjajevs
3. Service Manager	**[REMOVED]**
4. Program Manager	**[REMOVED]**

9.5.1.3 Plans and Procedures Used

Plans and Procedures Used:	
1. DRP	
2. Security Plan	

9.5.1.4 Assumptions

Assumptions:	
N/A	

9.5.1.5 Scope

Business Unit	System	Comments
All CUST-DEV2 units	All Servers	

9.5.1.6 Required Roles and Responsibilities

Duties & Responsibilities:	
Individual	**Duties**
[REMOVED]	He notes that the power is interrupted and informs the RIGA project Manager, [REMOVED]. He sends a message to all active users to save there work and to close all applications on the servers.
[REMOVED]	She checks if all active users have received the message and are closing the applications.
[REMOVED]	Executes a controlled log off.
[REMOVED]	She informs the service manager, [REMOVED]
[REMOVED]	He informs the program manegern [REMOVED], if the poweroutage takes more then 4 hours.
[REMOVED]	He informs the project managers of DG TAXUD, [REMOVED]
[REMOVED]	Starts the servers again after the power interruption is ended
[REMOVED]	Informs the Riga Project manager when the servers are up and running
[REMOVED]	Informs the project team that they can start their activities and informs the Service Manager.
[REMOVED]	Informs the Program Manager the recovery is finished
[REMOVED]	Informs DG TAXUD Project Managers that the CUST-DEV2 activities are up and running again.

9.5.1.7 Entry and Exit Criteria

Test Cycle	Entry	Exit
1	Active CUST-DEV2 business units	All CUST-DEV2 activities are up and running again

9.5.1.8 Dependencies and pre-test tasks

Task	Responsibility	Completed?
None		

9.5.1.9 Tasks to set-up the environment

Task	Timing	Completed?
None		

9.5.1.10 Execution of Disaster Recovery Process

Activity	Expected Results	Actual Results Observations	Owner	Success Yes/No	Comments
Controled Powerdown	No forced end of running applications		System and Telecommunications Lead		
Communication	All involved parties are informed		Service Manager		
Restart of servers	All CUST-DEV2 activities in the Riga DC are running		Riga Project Manager		

9.5.1.11 Post DR Test Tasks

Task	Timing	Completed?
Update the test plan if necessary		

Task	Timing	Completed?
Write the test report		

9.5.2 Unavailability of a project team member

9.5.2.1 General Information

Test Date:	To be completed
DRP Test Organized By:	Riga project Manager
Service Manager:	[REMOVED]
Test Conducted By:	Riga project Manager
Area Tested:	Unavailability of a project team member
Test Approved By:	Service Manager

9.5.2.2 Test Participants

Test Participants:	
1. Riga Project Manager	[REMOVED]
2. Two project team members	A team member who will be declared unavailable and a second team member who has been defined as backup of the first one.
3. Service Manager	**[REMOVED]**

9.5.2.3 Plans and Procedures Used

Plans and Procedures Used:	
1. DRP	
2. Security Plan	

9.5.2.4 Assumptions

Assumptions:	
N/A	

9.5.2.5 Scope

Business Unit	System	Comments
L'activity of the unaivalable resource	L'activity of the unaivalable resource	

9.5.2.6 Required Roles and Responsibilities

Duties & Responsibilities:	
Individual	**Duties**
[REMOVED]	She receives the information from the CUST-DEV2 Human Resources the message that resource will be unavailable. She informs the defined back-up resource to take over the as urgent defined activities of the unavailable resource.
[REMOVED]	The back-up resource has to find back the last versions of the activity related documentation
[REMOVED]	The back-up resource has to execute the activities
[REMOVED]	She has to check together with the 2 resources if the activities have been executed correctly and reports to the Service Manager, [REMOVED]

9.5.2.7 Entry and Exit Criteria

Test Cycle	Entry	Exit
1	Base line of the activities	Executed work

9.5.2.8 Dependencies and pre-test tasks

Task	Responsibility	Completed?
Define the resource who be be declared unavailable.	Riga project manager	
Define the activities in scope of the test	Riga project manager	

9.5.2.9 Tasks to set-up the environment

Task	Timing	Completed?
None		

9.5.2.10 Execution of Disaster Recovery Process

Activity	Expected Results	Actual Results Observations	Owner	Success Yes/No	Comments
Inform and help back-up resource getting started	Take over of the tasks by the back-up resource		Riga Project Manager		
Execute the tasks of the unavailable resource by the back-up resource	Correct execution of the tasks		Back-up resource		
Controle the correct execution of the tasks	All involved parties are informed		Riga Project Manager		

9.5.2.11 Post DR Test Tasks

Task	Timing	Completed?
Update the test plan if necessary		
Write the test report		

9.5.3

9.5.4 One of the servers is not available

9.5.4.1 General Information

Test Date:	To be completed
DRP Test Organized By:	Riga project Manager
Service Manager:	[REMOVED]
Test Conducted By:	Riga project Manager
Area Tested:	One server unavailable
Test Approved By:	Service Manager

9.5.4.2 Test Participants

Test Participants:	
1. Riga Project Manager	[REMOVED]
2. Systems and Telecom Team	[REMOVED]
3. Service Manager	[REMOVED]
4. Program Manager	[REMOVED]

9.5.4.3 Plans and Procedures Used

Plans and Procedures Used:	
1. DRP	
2. Security Plan	
3. FQP	
4. CQP SC02	

9.5.4.4 Assumptions

Assumptions:	
N/A	

9.5.4.5 Scope

Business Unit	System	Comments
All CUST-DEV2 units	The unavailable Server	

9.5.4.6 Required Roles and Responsibilities

Duties & Responsibilities:	
Individual	**Duties**
Rodions Sirjajevs, the systems and telecomunications lead	He notes that the server is no longer responding and informs the RIGA project Manager, **[REMOVED]**. His next action will be to try the restart of the server.

Duties & Responsibilities:	
Individual	**Duties**
[REMOVED]	She informs the team members of the unavailability of the server. If the action to restart the server does not succeed she also informs the Service Manager, [REMOVED].
[REMOVED]	If the restart does not succeed he contacts the maintenance contracter for a support intervention. He keeps the Riga project manager informed of the solution time.
[REMOVED]	Analyzes the activities impacted by the disaster and reports to the service manager.
[REMOVED]	Intervention to solve the problem. First he will give the service and telecommunications lead an estime of the time needed to solve the problem.
[REMOVED]	He informs the program manegern [REMOVED], if the poweroutage take more then 4 hours.
[REMOVED]	He informs the project managers of DG TAXUD, [REMOVED]
[REMOVED]	Agrees with DG TAXUD on which activity can be reduced if the server stays unavailable for more than 24 hours.
[REMOVED]	If server has be to replaced completly he starts the procurement procedure.
[REMOVED]	If server can be repared by the maintenance contracter and the server is running again the systems and communications lead will check if all data and application are still intact. If not he will restore the necessary back-ups.
[REMOVED]	Informs the Riga Project manager when the servers are up and running
[REMOVED]	Informs the project team that they can start their activities and informs the Service Manager.
[REMOVED]	Informs the Program Manager the recovery is finished
[REMOVED]	Informs DG TAXUD Project Managers that the CUST-DEV2 activities are up and running again.

9.5.4.7 Entry and Exit Criteria

Test Cycle	Entry	Exit
1	Active server in the Riga DC.	All CUST-DEV2 activities are up and running again

9.5.4.8 Dependencies and pre-test tasks

Task	Responsibility	Completed?
Define the server which will be used for the test	System and communication network lead and Riga project manager	
Define the impacted activities	Riga project manager	

9.5.4.9 Tasks to set-up the environment

Task	Timing	Completed?
Create a complete back-up of the server		

9.5.4.10 Execution of Disaster Recovery Process

Activity	Expected Results	Actual Results Observations	Owner	Success Yes/No	Comments
Server unavailable	Server operational without out loss of information		System and Telecommunications Lead and Riga Project Manager		

9.5.4.11 Post DR Test Tasks

Task	Timing	Completed?
Update the test plan if necessary		
Write the test report		

9.5.5 CUST-DEV2 offices in Riga unavailable

9.5.5.1 General Information

Test Date:	To be completed
DRP Test Organized By:	Riga project Manager
Service Manager:	[REMOVED]

Test Conducted By:	Riga project Manager
Area Tested:	CUST-DEV2 Riga office unavailable
Test Approved By:	Service Manager

9.5.5.2 Test Participants

Test Participants:	
1. Riga Project Manager	[REMOVED]
2. Service Manager	[REMOVED]

9.5.5.3 Plans and Procedures Used

Plans and Procedures Used:	
1. DRP	
2. Security Plan	

9.5.5.4 Assumptions

Assumptions:	
N/A	

9.5.5.5 Scope

Business Unit	System	Comments
All CUST-DEV2 units in RIGA	N/A	

9.5.5.6 Required Roles and Responsibilities

Duties & Responsibilities:	
Individual	**Duties**
Any team member	He notes that the offices are not accessible and he informs the Riga project manager, [REMOVED]. (he should use the contact list part he received in the welcome kit).
[REMOVED]	She informs all the users of the unavailability of the office and asks them to work from the other building or from home.

Duties & Responsibilities:	
Individual	**Duties**
[REMOVED]	She informs the service manager, [REMOVED]
[REMOVED]	He informs the program manager [REMOVED], if the offices are unavailable for more then 4 hours.
[REMOVED]	He informs the project managers of DG TAXUD, [REMOVED]
[REMOVED]	She checks if all team activities can be executed and reports to the Service Manager
[REMOVED]	Informs the Program Manager that the recovery is finished
[REMOVED]	Informs DG TAXUD Project Managers that the CUST-DEV2 activities running as should.

9.5.5.7 Entry and Exit Criteria

Test Cycle	Entry	Exit
1	Active CUST-DEV2 business units	All CUST-DEV2 activities are up and running as normal

9.5.5.8 Dependencies and pre-test tasks

Task	Responsibility	Completed?
None		

9.5.5.9 Tasks to set-up the environment

Task	Timing	Completed?
None		

1.

9.5.5.10 Execution of Disaster Recovery Process

Activity	Expected Results	Actual Results Observations	Owner	Success Yes/No	Comments
All Riga CUST-DEV2 activities	Activities are running as normal		Riga Project Manager		

9.5.5.11 Post DR Test Tasks

Task	Timing	Completed?
Update the test plan if necessary		
Write the test report		

9.6 Obtain Management Approval

The purpose of this step is to present the results of the test to the organization's management. These results will be used by management to determine if the recovery plan actually accomplishes all of the requirements and objectives set for the test. Any improvements or revisions recommended by the testing team should be approved by management and made at this time.

10 Appendix

10.1 Disaster Recovery Resources

10.1.1 Recovery Team

CUST-DEV2 Service Manager (Disaster Recovery Coordinator) : [REMOVED]	**Backup:** [REMOVED]
CUST-DEV2 Riga Project Manager: [REMOVED]	**Backup:** [REMOVED]
Systems and Network Administrator: [REMOVED]	**Backup:** [REMOVED]
CUST-DEV2 Security Officer [REMOVED]	**Backup:** [REMOVED]

10.1.2 System and Telecommunications Team

Lead : [REMOVED]	**Backup :** [REMOVED]

10.1.3 CUST-DEV2 Contractor's Management

Account Lead: [REMOVED]
Programme Manager: [REMOVED]

10.1.4 DG TAXUD representatives

Contract Management : [REMOVED]	**Backup :** [REMOVED]
Project Manager : [REMOVED]	**Project Manager:** [REMOVED]

10.2 Locations

10.2.1 Development and hosting location

CUST-DEV2 contractor has a team where the infrastructure is installed which location is in:

[REMOVED]

10.2.2 Offline backup storage location

[REMOVED]

10.2.3 Development Support Tools location

[REMOVED]