OWNER:	ISSUE DATE:	VERSION:
21	02/06/2010	2.01

TAXATION AND CUSTOMS UNION DG
ITSM

SUBJECT:

IT Service Continuity Plan for Commission IT Services

DLV.8.2.3.1.2

REF: ITS-IPLN-SC06-ITSCP-003 EVOLUTIVE MAINTENANCE

FRAMEWORK CONTRACT # TAXUD/2007/CC/088

SPECIFIC CONTRACT 06

Document History

Edi.	Rev.	Date	Description	Action (*)	Pages
0	01	13/01/2009	Master document created	I	All
0	02	14/01/2009	Implementation of QC comments	I	All
0	10	14/01/2009	Sent for review to DG Taxation and Customs Union (SfR)	I	All
0	11	16/02/2009	Processed DG TAXUD comments after SfR review	I/R	As req.
1	0	17/02/2009	Submit for SfA	I/R	As req.
1	01	19/02/2009	Re-SfA	R	As req.
1	10	29/05/2009	Evolutive maintenance submitted for review	I/R	As req.
1	20	17/06/2009	Evolutive maintenance submitted for acceptance	I/R	As req.
1	21	13/04/2010	Evolutive maintenance submitted to QC	I/R	As req.
1	22	14/04/2010	Implementation of QC comments	I/R	As req.
1	30	15/04/2010	Evolutive maintenance submitted for review	I/R	As req.
2	00	25/05/2010	Evolutive maintenance submitted for acceptance	I/R	As req.
2	01	02/06/2010	Re-SfA	I/R	As req.

(*) Action: I = Insert R = Replace

Table of Contents

1. INTRODUCTION 5
1.1 PURPOSE AND GOAL 5
1.2 APPROACH 6
1.3 STRUCTURE OF THIS DOCUMENT 7
1.4 REFERENCE AND APPLICABLE DOCUMENTS 8
1.4.1 Reference Documents 8
1.4.2 Applicable Documents 9
1.5 TERMINOLOGY 9
1.5.1 Abbreviations and Acronyms 9
1.5.2 Definitions 11
2. SCOPE OF THE PLAN 13
2.1 APPLICATIONS AND SERVICES 13
2.2 SYSTEM ENVIRONMENTS 14
2.3 GEOGRAPHICAL AREAS (SITES) COVERED 14
2.4 DISASTER AND THREAT TYPES 15
3. REQUIREMENTS AND STRATEGY 16
3.1 AVAILABILITY REQUIREMENTS AND CLASSIFICATION 16
3.2 SERVICE LEVEL OBJECTIVES 20
3.3 BUSINESS RECOVERY TIME OBJECTIVES 21
3.4 RECOVERY POINT OBJECTIVES 23
3.5 RECOVERY STRATEGY 24
4. RISK ANALYSIS, ASSESSMENT AND MANAGEMENT 28
4.1 DISASTER IMPACT AND SEVERITY CLASSIFICATION 28
4.2 RISK PROBABILITY ASSESSMENT 28
4.3 IDENTIFIED RISKS 30
4.4 PREVENTIVE MEASURES CURRENTLY IN PLACE 32
4.4.1 Utilities and HVAC Controls 32
4.4.2 Information System Controls 33
4.4.3 Information Security Controls 35
4.4.4 Data Protection Controls 36
4.4.5 Service Desk 37
4.5 PROPOSED RISK MITIGATION MEASURES 37
5. FURTHER ACTIONS TOWARDS IMPLEMENTATION 39
5.1 DISASTER RECOVERY PLAN (EXTERNAL DOCUMENT) 39
5.2 DISASTER RECOVERY TEST PLAN 39
5.3 STATUS ASSESSMENT RELEVANT BCP/DRP PLANS 40
5.4 GENERAL RECOMMENDATIONS AND NEXT STEPS 43
5.5 PLANNING 46

Table of Tables

Table 1-1: Document structure 7
Table 1-2: Reference documents 8
Table 1-3: Applicable documents 9
Table 1-4: Abbreviations and acronyms 10
Table 1-5: List of definitions 12
Table 2-1: List of applications and services in scope 14
Table 3-1: Continuity requirements of applications and services 19
Table 3-2: List of service level objectives 20
Table 3-3: List of recovery time objectives 22
Table 3-4: List of recovery point objectives 24
Table 3-5: Matrix with recommended recovery strategies 27
Table 4-1: List with impact and severity classifications 28
Table 4-2: List with probability classifications 29
Table 4-3: Risk probability assessment 30
Table 4-4: List with identified risks 32
Table 4-5: List of environmental controls 33
Table 4-6: List of information system controls 34
Table 4-7: List of information security controls 36
Table 4-8: List of data protection controls 37
Table 4-9: List with risk reduction measures 38
Table 5-1List with BCP/DRP status information 42

Table of Figures

Figure 5-1: Recovery process 43

1. Introduction

This is the Deliverable "ITS-IPLN-SC06-ITSCP-003 Evolutive Maintenance" identified in Specific Contract SC06 to Framework Contract TAXUD/2007/CC/C088, Work Package WP.8.2.3 deliverable DLV.8.2.3.1.2.

This IT Service Continuity Plan (ITSCP) includes a Risk Analysis, a Disaster Recovery Plan (DRP) and a deployment plan in line with the Continuous Service Improvement Program (CSIP). The DRP is an external document [RD8] broken down into several sections dealing with the organisational aspects, crisis management and encompasses the instructions and procedures that are to be followed during a major interruption in services to recover or continue the operation of systems, infrastructure, services or facilities, in order to maintain service continuity.

This IT Service Continuity Plan includes a Business Impact Analysis (BIA) in chapter 3. It makes an inventory of the applications and services. It lists the impact of a disruption and makes an estimation of the maximum allowable downtime (RTO) and acceptable loss (RPO).

1.1 Purpose and Goal

The purpose of this plan is to define and document the business requirements in order to develop and agree the appropriate continuity strategies. The strategy will be a balance between risk reduction measures and recovery options. This will form the base input required to develop a DRP and measures which provide the mechanisms to ensure recovery capabilities that are in line with the business requirements as defined with this document.

The goal of this document is to support the overall Business Continuity Management process by ensuring that the required IT services (including computer systems, networks, telecommunications, technical support and service desk) can be recovered within required and agreed business timescales.

The plan is structured in line with the following objectives:

1. Reduce business risks by minimising the impact on the business and operational interference in case of manifestation of a disaster;
2. Increase the ability to recover services efficiently, from an end-to-end business perspective, in order of business priority;
3. Facilitate a proactive (rather than reactive) approach to continuity management;
4. Reduce the duration of interruption of services (duration of downtime).

1.2 Approach

- This plan supports the first step in establishing the requirements and the strategy upon which the following stages, being implementation and operations, will be based;
- To be successful the IT service continuity plan must translate the reality of all services and related components into meaningful information. To reflect that reality, ITSM collected various continuity requirements (related to applications/services) based on documentation already available and interviews conducted with several contacts;
- The agreed final requirements, strategy and risk reduction measures form the basis for the further development and implementation of the technical infrastructure and the DRP;
- A first round of questions and interviews has been done with key representatives and contacts in order to gain an understanding of the current situation. Furthermore, information has been collected from various sources upon which the analysis of the existing situation and status of relevant plans has been conducted;
- The continuity requirements have been inventoried as much as possible from both an applications and services perspective (end-to-end) in the context of the current situation;
- To be able to develop an effective DRP the relations and dependencies between the assets, services and organisational elements involved in the continuity plan must be mapped through the use of a dependency model. The model will be developed and used during the next phase to identify and document all dependencies crossing organisation, functional, technical and process boundaries;
- The required asset inventory will be completed with the help of each and every organisation identified in this document as being an integral part of the plan being; DG TAXUD, DIGIT, CCN/TC and ITSM. Lists of assets not under the responsibility of ITSM will not be duplicated or maintained as part of this plan. This to prevent administrative overhead associated with maintaining similar asset lists by multiple providers. These will be maintained by the relevant providers through their applicable mechanisms.

1.3 Structure of this Document

The document is structured as follows:

Ref.	Description
Chapter 1	**Introduction** Provides the reader with an overview of the document characteristics such as purpose and structure. It also lists related documents, as well as the abbreviations, acronyms and definitions used in this document
Chapter 2	**Scope of the Plan** Provides an overview of the scope of the plan listing the applications, applicable locations.
Chapter 3	**Requirements and Strategy** Provides an overview of the recovery approach applicable to this plan and defines the damage assessment and impact levels.
Chapter 4	**Risk Analysis** Provides information covering the risks, the probability of a threat manifesting itself and includes the preventive measures currently in place in relation to the disaster and threat types included in the scope of this plan.
Chapter 5	**Further actions towards implementation** Contains information on the external DRP and on the disaster recovery test plan. Provides the reader with a reference pointer to the DRP. Documents the recommendations and the deployment plan.

Table 1-1: Document structure

1.4 Reference and Applicable Documents

1.4.1 Reference Documents

Id	Reference	Title	Date	Version
RD1	ITS-IGLO-ITSM	ITSM Glossary	N/A	V1.11
RD2	TMP-REF-DRL	TEMPO Disaster Recovery Plan (Life Cycle)	24/08/2006	V2.02-EN
RD3	TMP-GDL-DRP	TEMPO Disaster Recovery Plan (Guide)	24/08/2006	V2.01-EN
RD4	TMP-TEM-DRP	DG TAXUD A3 - TEMPO Disaster Recovery Plan (Template)	08/03/2005	
RD5	ITS-IFQP-SC01-Frame Work Quality Plan	Frame Work Quality Plan	23/03/2010	V1.04
RD6	ITSM-DLV8.6.1.3.1-Technical Infrastructure Reference	TAXUD Technical Infrastructure Reference	13/10/2008	V0.04
RD7	TMP-FAC-DCS	Data process and system classification Fact Sheet	12/09/2006	V1.3-EN
RD8	ITS-IPLN-SC06-ITSCP-003-DRP	IT Service Continuity Plan for Commission IT Services – DRP Evolutive maintenance	25/05/2010	V2.00
RD9	CCN-CSEC-BCP	CCN Business Continuity Plan	18/07/2008	EN1.00
RD10	CCN-CSEC-DRP-FR	CCN Disaster Recovery Plan	29/07/2008	EN1.10
RD11	CCN-CSEC-BCRA	CCN Business Continuity Requirements Analysis	18/01/2008	EN2.00
RD12	SCIT68 -SLA_	Service Level Agreement (VAT related systems)	14/03/2008	V3.00
RD13	TMP-REF-ITSCM	TEMPO ITSCM Reference Manual	05/02/2008	V 1.5

Table 1-2: Reference documents

1.4.2 Applicable Documents

Id	Reference	Title	Date	Version
A1	TAXUD/2006/AO-007	ITT for ITSM	25/07/2006	N/A
A2	TAXUD/2007/CC/088	Framework contract	04/05/2007	N/A
A3	TAXUD/2007/DE/117	Specific Contract 02	19/09/2007	N/A
A4	TAXUD/2008/DE/114	Specific Contract 04	30/06/2008	N/A
A5	TAXUD/2009/DE/115	Specific Contract 05	29/06/2009	N/A
A6	TAXUD/2009/DE/128	Specific Contract 06	30/10/2009	N/A

Table 1-3: Applicable documents

1.5 Terminology

1.5.1 Abbreviations and Acronyms

The reader is referred to the Glossary [RD1] for a list of the definitions used in this project for a better understanding of this document. A selection of abbreviations and acronyms is additionally provided here for ease of reading.

Abbreviation / Acronym	Description
CCN/CSI	Common Communications Network/Common System Interface
CCN/CT	Common Communications Network/Technical Centre
CMT	Crisis Management Team
CCT	Crisis Coordination Team
CSIP	Continuous Service Improvement Program
DRP	Disaster Recovery Plan
DRRT	Disaster Recovery Response Team
HVAC	Heating, Ventilating, and Air-Conditioning
ITSCM	IT Service Continuity Management
LAN	Local Area Network
RAID	Redundant Array of Independent Disks
RPO	Recovery Point Objective
RT	Recovery Team
RTO	Recovery Time Objective
SAN	Storage Area network
SLO	Service Level Objective

Abbreviation / Acronym	Description
SPOF	Single Point of Failure
UPS	Uninterruptible Power Supply
DG DIGIT	Directorate–General for Informatics
DG TAXUD	Directorate-General for Taxation and Customs Union
preSAT	Pre Site Acceptance Test
SAT	Site Acceptance Testing
CT	Conformance Testing
BCP	Business Continuity Plan
OLA	Operating Level Agreement

Table 1-4: Abbreviations and acronyms

1.5.2 Definitions

Term	Definition
Force Majeure	No Party shall be liable for any failure to perform its obligations where such failure is a result of a natural disaster (including fire, flood, earthquake, storm, hurricane or other natural disaster), war, invasion, act of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalisation, government sanction, blockage, embargo, labour dispute, strike, lockout or interruption or failure of electricity or telephone service.
Maximum tolerable period of unavailability	Duration after which an organisation's viability will be irrevocably threatened if product and service delivery cannot be resumed.
RPO	The Recovery Point Objective (RPO) is the point in time to which data must be recovered as defined by the business after manifestation of a disaster. This is generally a definition of what an organisation determines as an "acceptable loss" in a distressed situation.
RTO	The Recovery Time Objective defines the maximum acceptable downtime for a given application or system. It is the target time set for resumption of product, service or activity delivery after a major incident. The recovery time objective has to be less than the maximum tolerable period of unavailability.
Recovery Strategy	Approach by an organisation that will ensure its recovery and continuity in the face of a disaster or other major incident or business disruption.
Disruption	An event, whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), which causes an unplanned, negative deviation from the expected delivery of products or services according to the organisation's objectives.
Impact	Evaluated consequence of a particular outcome.
Invocation	Act of declaring that an organisation's business continuity plan needs to be put into effect in order to continue delivery of key products or services.
Disaster Recovery Plan	Clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the disaster management process.
Activity	A set of actions designed to achieve a particular result.
Disaster	A disaster, in the context of this document, is defined as a serious disruption in provided services that may result in an unacceptable level of damage and service unavailability, due to a series of possible events.
Business Continuity Plan	A documented collection of procedures and information developed compiled and maintained in readiness for use during a disaster to enable an organisation to continue to deliver its critical activities at an acceptable pre-defined level.

Term	Definition
IT Service Continuity Plan	A plan defining the steps required recovering one or more IT services. The plan will also identify the business requirements, the recovery strategies, triggers for invocation, people to be involved, communications etc. The IT service continuity plan should be part of the business continuity plan.
Business continuity management	A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Service Provider	An organisation supplying services to one or more internal or external customers. Service Provider is often used as an abbreviation for IT Service Provider.

Table 1-5: List of definitions

2. Scope of the Plan

2.1 Applications and Services

The scope of this plan includes the Commission IT services. It covers the Service Desk operations, the ITSM thread, the business threads which are hosted on the ITSM infrastructure and the applications hosted by DIGIT.

For the CCN applications and services (CCN Mail2 and CCN Gateway) the IT Service Continuity Plan is managed by CCN/TC and is out of scope of this deliverable.

The table below provides a list with the applications and services in scope of this plan including the service provider with initial ownership for delivery of continuity services for that particular application or services.

Business Thread/Service	Applications	Service Provider
ITSM	owITSM	ITSM
	E-mail (Ms Exchange)	ITSM
	ITSM Portal	ITSM
Excise	SEED	DIGIT
	PSP	ITSM
Customs	ART	DIGIT
	CN	DIGIT
	DDS	DIGIT
	CRMS	DIGIT
	EBTI	DIGIT
	ECICS	DIGIT
	EOS	DIGIT
	ISPP	DIGIT
	SMS	DIGIT
	SPEED-ECN	ITSM
	SURV2	DIGIT
	SUSP	DIGIT
	TARIC	DIGIT
	TARREP	DIGIT
	CSI Bridge/CMR	DIGIT
	HTTP Internet Bridge	DIGIT

Business Thread/Service	Applications	Service Provider
	QUOTA	DIGIT
	SMART	DIGIT
	CS/RD	ITSM
	CS/MIS	ITSM
	VIES Monitoring	ITSM
	VIES-on-the-WEB Monitoring	DIGIT
	VIES-on-the-WEB Configuration Tool	DIGIT
	VIES Statistics System	ITSM
	Taxes in Europe Database (TEDB)	DIGIT
	VIES-on-the-Web	DIGIT

Table 2-1: List of applications and services in scope

2.2 System Environments

Only production systems are in scope of this plan, preSAT, CONF and SAT are out of scope.

2.3 Geographical Areas (sites) Covered

Service Desk:

XXX

Data Centres:

ITSM

XXX

XXX

DIGIT

XXX

CCN/TC:

XXX

XXX

2.4 Disaster and Threat Types

This plan does not directly cover longer-term risks such as those from changes in business direction, diversification, restructuring, and so on. While these risks can have a material impact on IT service elements and their continuity mechanisms, identification and evaluation of these including risk mitigation through changes or shifts in business and IT strategies, are part of the Change Management program. Minor technical faults (for example, non critical disk failure) are out of scope, unless there is a possibility that these could have a major impact on the business. These risks are covered mainly through the Incident Management process, or resolved through the planning associated with the disciplines of Availability Management, Problem Management; and to a lesser extent through Change Management, Configuration Management and 'day to day' operational management.

It must be noted that these do not apply to DIGIT and CCN from a risk assessment perspective since both organisations have their own business continuity and risk management plans including measures to cope with major disruptions. This plan however does cover the organisational and procedural aspects for the recovery of services involving DIGIT and CCN/TC as result of a disaster.

The following provides an overview of the possible threats and disaster types in scope of the IT service continuity plan.

1. Force majeure

Force majeure is herewith defined as any failure as a result of natural disaster (including fire, flood, earthquake, storm, hurricane or other natural disaster), war, invasion, act of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalisation, government sanction, blockage, embargo, labour dispute, strike, lockout or interruption or failure of electricity or telephone service.

2. Information system failures

Significant outages caused by server equipment, application and software failures, loss of records and/or data, network equipment and circuit failures impacting Commission IT services.

3. Serious Information Security related threats

Significant outages caused by hostile attacks such as malicious code and network attacks (Intrusions or Denial of Service attacks), unauthorised electronic and physical access, and cyber crime.

4. Utilities and HVAC failures

The threats considered as part of this category include power outages, HVAC equipment failures, water leaks, fire, and power surges.

5. Acts of Organised Crime: any act of organised crime impacting Commission IT services.

3. Requirements and Strategy

3.1 Availability Requirements and Classification

The applications and services part of the scope of this plan are classified according to their level of integrity and availability. The classification levels used are those extracted from [RD7] and indicate the extent of criticality of the applications and services. The following is an extract from [RD7] documenting the classification levels and the definitions used.

- *MODERATE: This classification shall apply to information or information systems the loss of whose integrity or availability might threaten the internal working of the Commission;*
- *CRITICAL: This classification shall apply to information or information systems the loss of whose integrity or availability might threaten the position of the Commission with regard to other Institutions, Member States or other parties;*
- *STRATEGIC: This classification shall apply to information or information systems the loss of whose integrity or availability would be unacceptable to the Commission, to other Institutions, to Member States or to other parties.*

The table below provides the list of the applications and services currently in scope of this document including their availability requirements specified in continuous hours and the selected classification. For each of them, the following indications are provided:

- Availability requirements expressed in maximum tolerable period of unavailability; this is the duration after which an organisation's viability (either financially or through loss of reputation) will be irrevocably threatened if delivery of a particular product or service cannot be resumed;
- Availability classification (Moderate / Critical / Strategic) following [RD7] terminology.

The classification and availability requirements should be agreed by the sector leaders in cooperation with the ITSM business perspective manager during the implementation phase.

Application/ Service name	Availability Requirements (Maximum tolerable period of unavailability)	Availability Classification
SMART	Unavailability will have no critical impact on Member States or the Commission. The tolerated unavailability of the system is judged to be above 48 hours	Moderate
CS/RD	Unavailability will have an impact on critical processes, Member States and the Commission. The availability of CS/RD (Business Code lists and Customs Office Code lists) is Critical. The tolerated	Critical

Application/ Service name	Availability Requirements (Maximum tolerable period of unavailability)	Availability Classification
	unavailability of the system is judged to be between 3,5 hours and 48 hours.	
CS/MIS	It provides monitoring and handling of the NCTS operations, reporting on NCTS-related traffic (messages, NCTS Movements), reporting on NCTS resource utilisation, monitoring and handling of National applications unavailability - National Transit Applications (NTAs) and National Export Control Applications (NECAs). Unavailability will have a critical impact on Member States. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
owITSM	Unavailability of the IT service management tool will have no critical impact on Member States, the Commission or ITSM. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
E-mail (Ms Exchange)	Unavailability will have a critical impact on Member States, the Commission or ITSM. The tolerated unavailability of the system is judged to be between 3,5 hours and 48 hours.	Critical
ITSM Portal	Is used to access CS/RD. Unavailability will have critical impact on Member States, the Commission or ITSM. The tolerated unavailability of the system is judged to be between 3,5 hours and 48 hours.	Critical
PSP	Unavailability will have no immediate impact on Member States or the Commission. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
EOS	Unavailability will have an impact on Member States and citizens. The tolerated unavailability of the system is judged to be between 3,5 hours and 48 hours.	Critical
ART	Unavailability will have no critical impact on Member States. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
CN	The documents are managed through periods which are called publication cycles. The unavailability of the system is more critical when approaching the end of the cycle and should be between 3,5 hours and 48 hours.	Critical
DDS	Since this is a highly-visible public system, the tolerated unavailability of the system is judged to be very low. Unavailability will create a rather negative	Critical

Application/ Service name	Availability Requirements (Maximum tolerable period of unavailability)	Availability Classification
	image for the Commission. The tolerated unavailability of the system is judged to be between 3,5 hours and 48 hours..	
CRMS	The tolerated unavailability of the Community Risk Management System is judged to be between 3,5 hours and 48 hours.	Critical
EBTI	Unavailability can have an impact on the classification process in the Member States. The tolerated unavailability of the system is judged to be between 3,5 hours and 48 hours.	Critical
ECICS	Unavailability will have no critical impact on Member States or the Commission. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
ISPP	Unavailability of the system will have an impact on critical customs processes and the Member States. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
SMS	Unavailability can have an impact on the verification processes in the Member States concerning the authenticity of specimen. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
Surv2	The unavailability of the surveillance domain has no impact on critical customs processes but can have an impact on the effectiveness of the required monitoring processes. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
SUSP	Unavailability will have no critical impact on Member States or the Commission. The tolerated unavailability of the system is judged to above 48 hours.	Moderate
SPEED	The unavailability will have an impact on data exchange between EU and non EU countries. The tolerated unavailability of the system is judged to be between 3,5 hours and 48 hours.	Critical
TARIC	The unavailability of the system can have an impact on the declaration IT processes in the Member States. The tolerated unavailability of the system is judged to be between 3,5 hours and 48 hours.	Critical
TARREP	Unavailability will have no immediate impact on Member States or the Commission. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
QUOTA	The unavailability of the quota domain can have a	Critical

Application/ Service name	Availability Requirements (Maximum tolerable period of unavailability)	Availability Classification
	financial impact on the trader when longer than two days. The tolerated unavailability of the system is judged to be between 3,5 hours and 48 hours.	
SEED	The unavailability will have an impact on Member States Administrations. The tolerated unavailability of the system is defined in the Technical System Specification for SEEDV1 as follows: The maximum downtime must not exceed 3,5 hours during the business hours of the excise community (Monday-Friday, 05.00-23.00 CET).	Strategic
VIES Monitoring	Unavailability will have no immediate impact on Member States or the Commission. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
VIES-on-the-WEB Monitoring	Unavailability will have no immediate impact on Member States or the Commission. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
VIES-on-the-WEB Configuration Tool	Unavailability will have no immediate impact on Member States or the Commission. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
VIES Statistics System	Unavailability will have no immediate impact on Member States or the Commission. The tolerated unavailability of the system is judged to be above 48 hours.	Moderate
TEDB	The unavailability will have impact on Member States and the citizens. The tolerated unavailability of the system is judged to be less than 24 hours.	Moderate
VIES-on-the-Web	Unavailability will have impact on Member States and the citizens. The tolerated unavailability of the system is judged to be between 3,5 hours and 48 hours.	Critical

Table 3-1: Continuity requirements of applications and services

3.2 Service Level Objectives

The Service level objectives (SLO) during a disaster situation are described and listed in the table below. The minimum acceptable level of IT service and the maximum allowed time of operating at that level should be defined per IT environment. All standard service levels are suspended during an emergency situation.

Through close collaboration with service level management applicable service level objectives during a crisis situation must be established and agreed. The table below serves as an initial step for the ITSM hosted applications and ITSM provided services, it does not reflect reality. It is used merely as a guideline and example of possible targets, and will be formalised prior to the evolution of the continuity plan.

Business Thread	Application	SLO
Customs Taxation	CS/RD CS/MIS WEB2000 VIES Monitoring VIES Statistics System VIES-on-the-WEB monitoring	Minimum hours of service required. Critical periods of service, peaks, month-end, deadline processing, and so on. Less critical periods of service where downtime is more tolerable. Scheduled downtime periods for planned maintenance and upgrades. Capacity and performance targets. Availability targets. Maximum allowed time for operating at the above levels.
Services	**Application**	**SLO**
Service Desk	Not Applicable. This is a function.	Minimum hours of service required. Availability targets. Maximum allowed time for operating at the above levels.

Table 3-2: List of service level objectives

3.3 Business Recovery Time Objectives

This is the target set for recovering applications and services from a business perspective to allow business processes to be resumed within the maximum tolerable period of unavailability. Business recovery time objectives are usually determined by a business impact analysis (BIA) prior to a business continuity plan. However; ITSM was unable to use such an analysis as input and therefore took the initiative to establish the objectives based on information at hand. The suggested RTOs are within the limits imposed by the maximum tolerated unavailability and remain to be agreed by the sector leaders and business system owners in cooperation with the business perspective managers. The following suggested RTOs tiers are used:

Tier 1 - RTO of less than 3,5 hours

Tier 2 - RTO of 3,5 hours to 48 hours

Tier 3 - RTO of above 48 hours.

Business thread/Service	Application/ Service name	Recovery Time Objective
ITSM Thread	owITSM	Tier 3
	E-mail (Ms Exchange)	Tier 2
	ITSM Portal	Tier 2
Customs	ART	Tier 3
	CN	Tier 2
	DDS	Tier 2
	CRMS	Tier 2
	EBTI	Tier 2
	ECICS	Tier 3
	EOS	Tier 2
	ISPP	Tier 3
	SMS	Tier 3
	SPEED-ECN	Tier 2
	SURV2	Tier 3
	SUSP	Tier 3
	TARIC	Tier 2
	TARREP	Tier 3
	CSI Bridge/CMR	Tier 2
	QUOTA	Tier 2

Business thread/Service	Application/ Service name	Recovery Time Objective
	SMART	Tier 3
	CS/RD	Tier 2
	CS/MIS	Tier 3
Excise	PSP	Tier 3
	SEED	Tier 1
Taxation	VIES Monitoring	Tier 3
	VIES-on-the-WEB Monitoring	Tier 3
	VIES-on-the-WEB Configuration Tool	Tier 3
	VIES Statistics System	Tier 3
	TEDB	Tier 3
	VIES-on-the-Web	Tier 2

Table 3-3: List of recovery time objectives

3.4 Recovery Point Objectives[1]

Due to lack of standard recovery point objectives imposed by the Commission at this time, the complexity and extensive efforts required for determining these, both from a technological and organisational perspective, the following RPO tiers have been defined At this stage some RPO are still not applicable (N/A).

Tier 1 – RPO of 12 hours to 24 hours for critical applications
Tier 2 – RPO of 24 hours to 120 hours for moderate applications

Business thread/Service	Application/ Service name	Recovery Point Objective
ITSM Thread	owITSM	Tier 2
	E-mail (Ms Exchange)	Tier 1
	ITSM Portal	Tier 1
Customs	ART	Tier 1
	CN	Tier 1
	CRMS	Tier 1
	DDS	Tier 1
	EBTI	Tier 1
	ECICS	Tier 2
	EOS	Tier 1
	ISPP	Tier 2
	SMS	Tier 2
	SPEED	Tier 1
	SURV2	Tier 2
	SUSP	Tier 2
	TARIC	Tier 1
	SMART	Tier 2
	CS/RD	Tier 1
	CS/MIS	Tier 2

[1] The implementation of the suggested recovery point objectives applicable to the applications hosted and housed by DIGIT and services provided by CCN/TC must be confirmed and realised in co-operation with both service providers. ITSM is not in the position to impose these upon any provider other then for those systems hosted and applications managed by ITSM.

Business thread/Service	Application/ Service name	Recovery Point Objective
	TARREP	Tier 2
	QUOTA2	Tier 1
	CSI Bridge/CMR	Tier 1
Excise	PSP	Tier 2
	SEED	Tier 1
Taxation	VIES Monitoring	N/A
	VIES-on-the-WEB Monitoring	N/A
	VIES-on-the-WEB Configuration Tool	N/A
	VIES Statistics System	N/A
	TEDB	Tier 2
	VIES-on-the-Web	N/A

Table 3-4: List of recovery point objectives

3.5 Recovery Strategy[2]

Different services within the organisation require different built-in resilience and different recovery options. What ever option chosen, the solution must be aligned to the requirements and the business recovery time objectives. As a general rule, the longer the business can survive without a service, the cheaper the solution is.

This section of the document describes the various recovery options available and includes a matrix with the selected options per application and services in scope of this plan. The selected options are based on the classification of the applications as defined in section 3.1, the RTO in section 3.3 and the RPO in section 3.4.

[2] The implementation of the suggested recovery strategies applicable to the applications hosted and housed by DIGIT and services provided by CCN/TC remains to be confirmed by and realised in corporation with both service providers. ITSM is not in the position to impose these upon any provider other then for those systems hosted by and services provided by ITSM.

Manual recovery
For some services manual recovery can be an effective measure for a limited time frame until the IT service is resumed. For instance, a Service Desk call logging service could survive for a limited time using paper forms linked to a laptop computer with a spreadsheet.

Gradual recovery
This option (sometimes referred to as 'cold standby') is applicable to applications that do not need immediate restoration of business processes and can function for a period of above 48 hours, or longer, without a re-establishment of full IT facilities. This may include the provision of empty accommodation fully equipped with power, environmental controls and local network cabling Infrastructure, telecommunications connections, and available in a disaster situation for installation of computing equipment. Supporting hardware can be either remaining capacity at a second data centre or hardware available via drop ship arrangements with a third-party vendor. A best effort recovery objective with no pre-determined recovery time frame is applicable.

Intermediate Recovery
This option (sometimes referred to as 'warm standby') is selected by organisations that need to recover IT facilities within a predetermined time to prevent impact to the business process. This typically involves the re-establishment of the critical systems and services within a couple of days, between two and five days.

This involves the use of a second data center with production running at one site, and test and development running at the other. Test and development equipment takes on a production role in the event of a disaster. Delays may be encountered while the site is re-configured and the applications and data restored from backups.

Fast Recovery
This option (sometimes also referred to as ‘hot standby’) provides for fast recovery and restoration of services within a 3,5 hour period. It includes systems, applications and communications already available and configured, and data mirrored from the operational servers. Recovery and switch over to the backup site is accomplished with little loss of service. This requires additional equipment to the operational one.

Immediate Recovery
This option, sometimes referred to as 'hot standby and/or mirroring', provides a high degree of fault tolerance with virtually no impact to the end user and the business if the system goes down

Replication and synchronisation is part of the design of the system/application. Sufficient equipment will be dually located in two locations to run the complete service from either location in the event of loss of one facility. The lost facility can then be recovered whilst the services are provided by the other location.

The matrix below provides an overview of the selected recovery strategies per application based on the analysis and the conclusions drawn earlier in this document.

Application/ Service	Manual Recovery	Gradual Recovery (>48hrs)	Intermediate Recovery (3,5hrs-48hrs)	Fast Recovery (<3,5hrs)	Immediate Recovery (real-time)
SMART		X			
CS/RD			X		
CS/MIS		X			
CRMS			X		
owITSM			X		
E-mail (Ms Exchange)			X		
ITSM Portal			X		
PSP			X		
EOS			X		
ART			X		
CN			X		
DDS			X		
EBTI			X		
ECICS		X			
ISPP		X			
CRMS			X		
SMS			X		
Surv2		X			
SUSP			X		
TARIC		X			
TARREP		X			
QUOTA2			X		
Service Desk[3]	X		X		
SPEED			X		
SEED			X		
CSI			X		

[3] Several options have been selected for the Service Desk because the initial recovery of Service Desk operations can start with a manual work around while the intermediate recovery strategy is being executed.

Application/ Service	Manual Recovery	Gradual Recovery (>48hrs)	Intermediate Recovery (3,5hrs-48hrs)	Fast Recovery (<3,5hrs)	Immediate Recovery (real-time)
Bridge/CMR					
HTTP Internet Bridge		X			
VIES Monitoring		X			
VIES-on-the-WEB Monitoring		X			
VIES-on-the-WEB Configuration Tool		X			
VIES Statistics System			X		
TEDB			X		
VIES-on-the-Web			X		

Table 3-5: Matrix with recommended recovery strategies

4. Risk Analysis, Assessment and Management

Estimation of likelihood and impact is not an exact science. The impact estimates in this chapter are based on envisaged scenarios of what "might happen" and probability estimates are based on historical information that such a scenario has happened under similar conditions, knowing that circumstances will never be exactly the same.

This section covers a risk analysis applicable to the ITSM Infrastructure at the XXX and XXX data centres and to the XXX Service Desk in XXX. DIGIT has conducted a risk analysis as part of their BCP project which is not published or available to the public. Therefore, no details are included in this document applicable to possible risks identified at DIGIT. Upon request an audit may be performed. Risk assessment information pertaining to CCN could not be obtained either. General recommendations for mitigation of possible risks, if applicable, on an organisational and procedural level with regards to DIGIT and CCN are however included in section 5.4.

4.1 Disaster Impact and Severity Classification

This section defines the impact and corresponding severity levels on delivered services. It is used as a guideline to classify the severity and define the impact of a major disruptive event. The impact is expressed in understandable business terms and gives an indication of the unavailability of services as a result of the severity of the situation. The severity levels are expressed using a Low, Medium to High scale, presented in Table 4-1.

Impact	Severity Classification
ITSM services are unavailable or unstable for more than 48 hours	High
ITSM services are unavailable or unstable for 24 hours to 48 hours	Medium
ITSM services are unavailable or unstable for less than 24 hours	Low

Table 4-1: List with impact and severity classifications

4.2 Risk Probability Assessment

The risk occurrence probability is expressed using a linear scale (Low, Medium, High) and reflects the likelihood of one or more threats occurring over a two-year period based on actual experience within ITSM.

Probability Description	Classification
Happens several times per year within our company, >= 5 occurrences	High
Incident has occurred within the company, from 1 to 5 occurrences	Medium
Heard of in the industry or occurs < 1 time	Low

Table 4-2: List with probability classifications

This assessment is applicable to the XXX and XXX ITSM data centres and to the XXX Service Desk. Table 4-3 below presents the probability of occurrence and the impact assessment performed on the risks introduced by the threats.

Category	Threat	Probability	Impact
Natural Disaster	Hurricane	Low	High
	Flood	Low	High
	Snowstorm	Low	High
	Earthquake	Low	High
	Freezing Conditions	Low	Medium
Information Systems	Computing equipment failures	Medium	Low
	Software failures	Medium	Low
	Application failures	High	Low
	Loss of records or data	Low	Low
	Network equipment failures	Medium	Low
	Leased line failures	Medium	Low
Information Security	Intrusions or Denial of Service attacks	Low	Medium
	Malicious code such as viruses, worms or Trojan horses	Low	Medium
	Unauthorised electronic access	Low	Medium
	Unauthorised physical access	Low	Medium
	Cyber Crime	Low	Medium
Acts of Organised Crime	War	Low	High
	Arson	Low	Low

Category	Threat	Probability	Impact
	Theft	Low	Low
	Sabotage	Low	Medium
	Terrorism	Low	High
Utilities and HVAC	Electrical Power Outage	Medium	High
	Water leaks	Low	Medium
	HVAC malfunction	Medium	Medium
	Power surge	Low	Medium

Table 4-3: Risk probability assessment

4.3 Identified Risks

Category	Service provider	Ref	Risk
Information Systems (Network Infrastructure)	ITSM	R1	There is currently no backup line in place for the Internet connection at the XXX Data Centre. All Internet communications is currently supported by a single circuit, delivered by a single supplier. This is a single point of failure (SPOF) that can be addressed using backup and failover mechanisms.
	ITSM	R2	Six local area network (LAN) switches that provide network connectivity to the servers, firewalls and network equipment, are currently in production. Most of these switches are currently configured in single mode and form within each LAN segment-a SPOF. Spare LAN equipment is available at XXX. No automatic failover mechanisms exist for the following: Internet LAN connection, CCN LAN connection, DIGIT LAN connection. This approach is receptive to outside influences such as weather and traffic conditions and does not guarantee a swift switch over.
	ITSM	R3	The Internet router is currently a SPOF. It is a single router, with only one power supply and is not setup within an automatic failover configuration. A spare router does exist at XXX however; upon hardware failure a manual switch over must occur. This approach does not guarantee a swift switch over and is receptive to outside influences such as weather and traffic conditions.

Category	Service provider	Ref	Risk
	ITSM	R4	There is a Juniper firewall currently in production in XXX and used by the Service Desk to establish connectivity to the XXX data centre. There is spare equipment at the XXX facility and a manual switch over procedure used in case of equipment failure. However, no automatic failover capabilities exist at this stage. There is a dependency on resources at these sites to perform the switch over. This can be considered a risk and does not guarantee continuity within a defined time frame.
Information Systems (Systems Infrastructure)	ITSM	R5	The EMC Storage Area Network (SAN) is used to store server images, databases and critical configuration files required by servers and applications. Applications belonging to the e-Customs, Customs, Excise and Taxation business thread including the ITSM thread have a critical dependency on the EMC based SAN. Even tough the SAN has extensive redundancy built in; the chassis and the back plane remain critical SPOF's and pose a serious risk to the continuity of services.
	ITSM	R6	Databases are currently not configured in a cluster with automatic failover capabilities. They are stored on a single SAN array which does not include a clustered failover solution and is considered a major SPOF.
	ITSM	R7	The XXX Escala AIX production server is currently not configured within a clustered solution that facilitates automatic failover. When required, depending on the severity of the situation, a manual switch over to the test server is invoked however; there are currently no formal procedures in place to facilitate this.
Natural Disasters	ITSM	R9	No recovery strategy has been defined or implemented at his stage in terms of recovery measures such as a hot-standby location and/or computer room at an alternate site to enable the recovery from possible natural disasters that may result in a loss of the data centre or site premises for an extended period of time.
Acts of Organised Crime	ITSM	R10	No recovery strategy has been defined or implemented at his stage in terms of recovery measures such as a hot-standby location and/or computer room at an alternate site to enable the recovery from possible disasters that may result in a loss of the data centre or site premises for an extended period of time.

Category	Service provider	Ref	Risk
Documentation and media	ITSM	R11	Copies of documentation and software media are not stored at an offsite location. Documentation and media is stored at the XXX data Centre. There are currently no provisions to safeguard media and documentation against loss.
AV measures	ITSM	R12	There are currently no AV measures implemented for Solaris, AIX and Linux servers. This introduces certain vulnerabilities that can be exploited by malicious code. The risk factor however is very low due to the fact that most malicious code targets Windows servers.

Table 4-4: List with identified risks

4.4 Preventive Measures Currently in Place

Preventive measures include the measures implemented to prevent the probability of a threat manifesting itself and minimise the implications caused by manifestation of a threat. These are pro-active in nature and include elements such as: fire distinguishers, use of inflammable materials, appropriate cooling, use of redundant and fault tolerant systems and backup procedures, temporary transfer of activities to another location for the Service Desk.

4.4.1 Utilities and HVAC Controls

This table presents an overview of the applicable ITSM measures and controls for utilities and HVAC currently in place.

Item	Measures
HVAC	Units with built in resilience and under floor cooling maintain room temperature at industry standards (21 degrees) and humidity at 50% with a cooling load per rack of 2.5KW.
Fire	The latest technology in fire control and automated early warning environmental alarm system (VESDA) is implemented. A system with based on detection of fire, smoke and differential changes in temperature and humidity levels is combined with a thermal detection system. When fire is detected the detection system controls the fully redundant gas suppression.
Water leaks/flooding	A water detection system is implemented and is based on a “room-in-a-room” concept with sensors in between. When water is detected, early steps can be taken before water enters the main computer room.

Item	Measures
Electrical outage and Power surges	Facilities are designed with fault tolerant power supply including fully redundant dial power feeds to equipment racks. Power feeds are backed up by a dual UPS system (Uninterruptable Power Supply) and diesel generators that keep each system running indefinitely without direct electric grid power. However the power outage of December 2009 demonstrated that the fault tolerant system cannot be 100% guaranteed.
Data protection	The current tape storage procedure includes the storage of cloning tapes at an off-site location,

Table 4-5: List of environmental controls

4.4.2 Information System Controls

This table presents an overview of the ITSM applicable measures and controls currently in place to prevent possible service interruptions caused by information system failures.

Item	Measures
Virtual Servers	Linux and Windows servers can be redistributed through VM-Ware's VMotion, so that applications are distributed to other virtual servers in case a (virtual) machine crash occurs.
Physical Servers	Multiple Fujitsu XXX RX300 Wintel servers are configured within a VMware cluster with automatic failover capabilities. Fujitsu SPARC T5220 servers are configured within a cluster using Zone technology with manual failover capabilities. Upon failure support staff can, within a few minutes upon detection, reload virtual servers to another physical server. Servers are fully redundant and contain dual hardware components such as controllers, network cards, CPU and power supplies. Dual fibre host bus adapters provide redundant connectivity to the SAN.
Hard drives	RAID 10, RAID 1 and RAID5 arrays are used as the standard technology. This decreases the likelihood of service interruptions caused by hard drive failures.
Databases	Databases are stored on the SAN with RAID10 configured drives and backed up to tape as per the backup procedure. See data protection for backup procedures

Item	Measures
Software and Applications	Complete server images are stored on the file server and backed up on a weekly basis. These are an identical copy of the servers including the configuration of the Operating system and application. Network equipment configuration files are backed up to a central location on the network.
Storage Area Network (SAN)	The EMC Clarion CX3-40F is fully redundant. It contains dual components such as controllers, multiple CPUs, fibre channels and redundant power supplies. Dual SAN switches with automatic failover capabilities provide interconnectivity between servers and the SAN. Dual fibre connections between the SAN switch and the Storage Array ensures redundant connectivity and automatic failover capabilities. Each server making use of the SAN is connected via dual fibre optic cables.
Router	There is a spare Internet router at XXX. Upon router failure detection and when required (depending on the severity of the situation), a recovery procedure is invoked to manually replace the defective hardware.
LAN Cabling	LAN cabling is redundant. Dual fibre cables are connected to each LAN switch.
Firewalls	Spare equipment for the Checkpoint and PIX firewall is available at XXX. Upon failure detection and when required (depending on the severity of the situation), a replacement procedure is invoked to manually replace the defective hardware.
LAN switches	There are six LAN switches currently in production, connecting the different LAN segments. The LAN segment with the production servers has dual switches with automatic failover. High availability protocols and mechanisms such as spanning tree and trucking are used to facilitate automatic failover. Spare LAN equipment is available at XXX in case of equipment failure.

Table 4-6: List of information system controls

4.4.3 Information Security Controls

This table below presents an overview of the ITSM security measures and controls currently in place.

Item	Measures
Electronic Access	Electronic access to networked workstations is only allowed to authorised users through the use of username and password. Passwords may be no shorter than 7 (seven) characters, and must meet complexity requirements enforced by the policy. It is mandatory to change the log-on password every 90 days. The last three used passwords are not allowed to be used. To provide resistance to "brute force" password guessing attacks, domain accounts are automatically locked-out after five unsuccessful log-on attempts and may only be un-locked through the manual intervention of an administrator or after fifteen minutes. Electronic access to servers is only allowed to authorised users through the use of administrator accounts/passwords. A domain password policy is implemented with stringent controls. The policy enforces a minimum password length and an expiration of 90 days. In addition a minimum set of characters is enforced and passwords must meet stringent complexity requirements. Windows domain controllers are used to authenticate users and assign access tokens based on user privileges. Functional managers must follow a procedure and approve access for their staff prior to the system administrator granting system access to users. A form, which must be signed by the requesting functional Manager, is used to record all relevant user details prior to granting access. The Checkpoint, PIX and Watch guard firewalls are used to control network access based on access control lists.

Item	Measures
Physical Access	The data centre facility is equipped with a comprehensive security infrastructure. The following lists the various controls in place: • Entrance door with air-lock and audible alarm; • Timers to prevent doors being left open; • External and internal CCTV monitoring and recording • Key card access; • Steel plated doors between different areas (public, customer, power control access between areas; • Access-zones allowing one individual to enter at a time. Security guards are present 24 hours. A comprehensive access request procedure ensures that all access is approved and controlled by ITSM. Once access has been approved by ITSM internal security, personnel must use valid identification at the security guards prior to obtaining access.
Malicious code	Trend Micro anti-virus software is used on all Windows servers. A virus signature distribution server checks for new updates on the Internet continuously and pushes any new updates to servers instantaneously upon detection of a new version. Servers also check the distribution servers for new updates constantly. Workstations use AVAST for virus protection and use an automatic update mechanism to download and update virus signature files.
Intrusions detection and/ or Denial of Service attacks	The Checkpoint firewall used at the edge of the Internet border is used to guard against threats such as intrusion or denial of service attacks through the use of smart defence. There is no host based IDS installed on servers.
Security Governance Framework	The Security Governance Framework governs all security issues at ITSM. This process is carried out within the Security Steering Committee. The Security Steering Committee is installed and chaired by the ITSM Project Director. Refers to SEC 1.1 in RD5

Table 4-7: List of information security controls

4.4.4 Data Protection Controls

Loss of data due to logical outages will cause interruptions in service. Logical outages are those associated with retrieving data due to object deletion, data corruption, backing out incorrect program changes, loss of printouts/reports, accidental deletion of files or data, etc. These could be the result of an accident, negligence, or intentional action. To protect and recover from such occurrences, there should be defined tape backup procedures and a policy.

This table below presents an overview of the ITSM applicable data protection measures and controls currently in place.

Item	Description
Backup retention	Tapes are retained for one month and then overwritten.
Backup types	One full tape backup each week. One incremental tape backup per day. Databases are backed up on-line via Oracle tools and stored on tape once per day. Transaction logs are backed up to tape twice per day.
Application and system software	Application and Infrastructure server images are stored on the file server. These images are backed up to tape once a week.
Tape storage	Tapes are currently stored on-site at the XXX data centre in the tape library. Weekly backups are cloned and stored externally in a cupboard in the ITSM Infra premises at XXX.
Data loss	RAID arrays are used to protect against data loss caused by hard drive failures.

Table 4-8: List of data protection controls

4.4.5 Service Desk

This table presents an overview of the possible ITSM measures for the continuity of the Service Desk activities

Item	Measures
Call handling	In case of a crisis with a prolonged outage in XXX premises the critical calls can be handled from a remote site either from Luxembourg either from remote workstations. Limited authorised personal will have access to the email system (ITSM Support mailbox) and to the Service Management Tool (owITSM).

4.5 Proposed Risk Mitigation Measures

The below proposed risk mitigation measures apply to the applications hosted on the ITSM Infrastructure and in scope of this plan.

Ref.	Description
RM1	The implementation of an additional Internet data communications circuit, if possible provided by an alternative telecommunications provider and physically connected using an alternate demarcation point, is recommended to facilitate service continuity. This will

Ref.	Description
	provide for additional protection and failover in case a severe disruption occurs due to manifestation of a threat.
RM2	It is recommended to implement dual switches within each of the various LAN segments, or at least for the LAN segments connecting all production servers and critical equipment to the LAN backbone. This will facilitate automatic failover and increase availability.
RM3	Development and implementation of a comprehensive backup procedure aligned to the defined business requirements and chosen recovery strategy, which includes a daily, weekly, monthly and a yearly backup cycle; including tape storage procedures using an alternative site to store tapes at. This must include regular removal of data from the main Data Centre to a suitable secured off site storage location. This will ensure retrieval of data following major disasters.
RM5	Implementing a SAN failover cluster with an additional EMC storage array with an identical disk configuration is recommended to mitigate the current identified SPOF. The final configuration and used mirroring technology however depends on the chosen recovery strategy. Due to the critical nature of the SAN and the fact that all applications depend on it, it is recommended to use an alternative location for the second SAN and apply an immediate or fast recovery strategy to facilitate high availability and continuity assurance.
RM6	The Juniper firewall located at XXX should be implemented within an automatic failover configuration to mitigate the risk associated with the unavailability of resources required to perform the manual switch over.
RM7	Installing additional power supplies on all LAN switches will increase the assurance of continuity during power outages due to automatic switch over to electrical power supplied by the UPS's at the Data Centre.
RM8	There are currently no AV measures in place for Solaris, AIX and Linux. There are several measures and options possible to mitigate the risks associated with this vulnerability. For all three environments the security patch levels of the kernel must be maintained and updated frequently, at a minimum once a year. This will require assessments to be conducted by security management and the appropriate tests to be done in conjunction with application management prior to deploying patches. In addition, for Linux appropriate AV software should be installed.

Table 4-9: List with risk reduction measures

5. Further actions towards implementation

The current status of the ITSM IT service continuity plan gives a solid foundation for further development. It presents a thorough coverage of aspects that need to be addressed in the continuity plan. The next evolution of the plan will provide additional considerations, recommendations and guidelines for continuity and contingency plans.

5.1 Disaster Recovery Plan (external document)

A critical part of handling any serious emergency situation is a DRP. The priority of the DRP is the minimisation of the emergency itself, the removal or minimisation of the threat of further damage and the re-establishment of external services such as power, communications, water etc. It forms a sub-component of the continuity plan and provides a written set of instructions directing the computer systems recovery process, in the event of an interruption in continuous service resulting from a disaster.

The ITSM DRP due to the criticality and complexity of its nature and scope is presented in a separate document, the ITSM Disaster Recovery Plan for Commission IT Services [RD8]. The description in DRP document is a limited DRP strategy, based on the current infrastructure and location. It provides a good overview of the contents of the DRP and the structure. It aims to focus on how to handle and recover from an emergency situation, and also the notification and reporting process during a crisis. The DRP will also cover organisational issues that need to be in place so the ITSM organisation, and any other involved service providers can handle a potential disaster which is in line with business expectations formulated in this continuity plan.

The DIGIT and CCN/TC DRP's are partners of this plan. These are not a direct result of this deliverable but form an extension of the IT service continuity plan for Commission IT services.

5.2 Disaster Recovery Test Plan[4]

The disaster recovery test plan and relevant procedures are addressed in a separate document which is part of deliverable DLV.8.2.3.1.4.1. The test plan describes the activities for testing the effectiveness and efficiency of the ITSM DRP taking into account, most of the time, the most likely disaster recovery scenarios; it will also describe the expected results including the expected time to recover each IT system and application in scope of this plan. It covers all activities required to train the DRRT and other stakeholders in order to be able to use and test the DRP and the DR procedures.

The key objectives of the test plan are:

[4] This is part of a separate deliverable and may be addressed as part of SC02 and SC04 which will be determined at a later stage.

- Exercise the recovery processes and procedures;
- Familiarise staff with the recovery process and documentation, and ensure that all relevant personnel are aware of the relevance and importance of their IT service continuity management activities and how they contribute to the achievement of the objectives;
- Verify the effectiveness of the recovery documentation;
- Verify the effectiveness of the recovery site;
- Establish if the recovery objectives are achievable and identify improvements to the DR strategy, infrastructure, and recovery processes;
- Raise, enhance and maintain awareness;
- Develop response emergency skills and competence throughout the ITSM organisation through active participation in exercises.

5.3 Status Assessment Relevant BCP/DRP Plans

This section describes at a high level the status of some BCP/DRP items in applicable to ITSM, DIGIT and CCN/TC. It is not based on any specific reference model or stipulated strategy. Neither does it provide an extensive analysis of every aspect of IT service continuity management or assess the maturity of existing plans and processes. This goes beyond the scope of this assessment.

The results of this assessment are based on the documentation received and reviewed, and interviews conducted with several resources. For those items relevant to ITSM, a more thorough analysis was conducted of which the results are included in this overall plan.

Interpretation of the information in this section might not always align to reality due to the inconsistent use of terminology and methodologies used between the various parties being ITSM, DIGIT and CCN/TC. The reader of this document is therefore encouraged to always refer back to the reference documents, if available, for a correct interpretation of the information in relation to the methodology and terminology used.

ID	Item description	ITSM	DIGIT	CCN
S1	Business/IT Service Continuity Plan existence.	IT service continuity plan (DLV 8.2.3.1.1) has been developed and submitted to TAXUD for approval.	Business continuity plan due end Q1/2009.	Business continuity plan exists.
S2	Risks assessment status.	Risk	Yes. Details	Unable to

ID	Item description	ITSM	DIGIT	CCN
		assessment results included in IT service continuity plan.	not published.	determine.
S3	Application of availability classifications and requirements.	Yes. Included in IT service continuity plan for Commission IT Services (based on TMP-FAC-DCS.)	Yes. Requirements and classifications are based on SEC (2006) 898 & 899	Yes. Requirements and classifications are based on draft commission decision concerning the security of information systems intended to replace decision C(95) 1510 on the security of information systems.
S4	Recovery strategy(s) defined and documented.	Yes.	Yes.	Yes.
S5	Recovery time objectives defined and included in plans.	Documented in this document.	Yes. Not published and not in line with the proposed objectives in the proposed ITSM IT service continuity plan for commission IT services.	Unable to determine.
S6	Disaster recovery plan.	The development of the DRP is part of the next phase of the project.	Yes. These are referred to as SOP's.	Yes.
S7	Test plan.	Covered by a RfE nr 166	Tests would be planned in	Yes. Is part of the business

ID	Item description	ITSM	DIGIT	CCN
			2010. No copy yet available of the test plan.	continuity test plan.
S8	Training plan.	Will be developed as part of the next phase of the project.	Training plan exists. No copy available.	Yes. Is part of the business continuity plan.
S9	Recovery procedures.	Part of the proposed DRP.	Recovery procedures are part of SOP's.	Part of Business Continuity Plan.

Table 5-1List with BCP/DRP status information

5.4 General Recommendations and Next Steps

Continuity and disaster recovery plans can be defined as a set of specialised organisational, technical and operational capabilities that enable agreed IT services to be recovered within agreed business timescales. These capabilities take the form of functions, resources, service assets, processes and procedures. The act of transforming these capabilities of the involved service providers into an integrated system is at the core of the IT service continuity plan for Commission IT services. A critical success factor in accomplishing this transformation is the use and application of one cohesive disaster recovery process that crosses organisational boundaries supported by common standards and streamlined procedures.

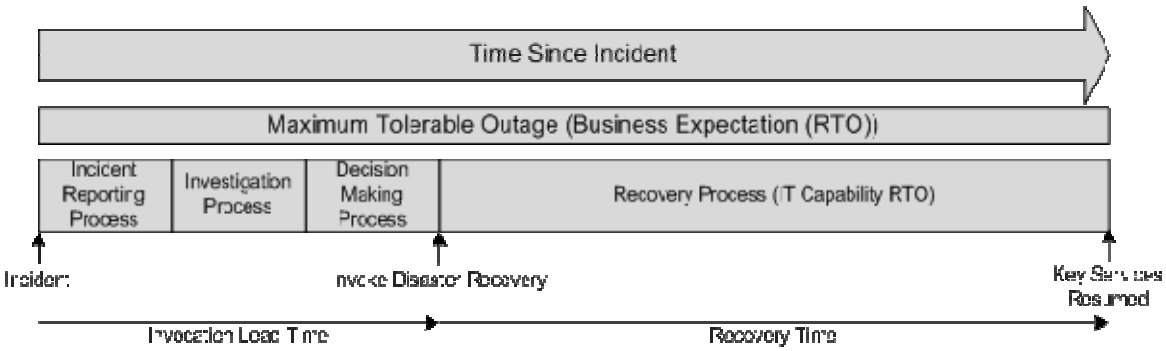

Figure 5-1: Recovery process

The figure above illustrates at a high level a disaster recovery process and the correlation between the incident starting, the reporting process, the investigation process, the decision making process, and the recovery process. It demonstrates the importance of an integrated approach to achieving the desired business results. With multiple service providers involved, it becomes extremely important to address certain aspects in order to achieve the implementation of such a cohesive recovery process in order to meet established business requirements. At a minimum the following aspects should be addressed:

- Business recovery time objectives;
- Information Technology recovery time objectives;
- Service Level Objectives;
- The use of standard classifications;
- Clearly defined roles and responsibilities;
- Functional, technical and procedural dependencies.

As long as the above aspects are not clearly defined, there is a risk of either creating a “gap” or an “overlap” between the recovery plans of the involved service providers, also referred to as actors, hence making recovery plans and processes absolutely inefficient. To avoid such a situation and creating the conditions of an effective application of the

IT service continuity plan, there is a need to address its "interfacing" and the aspects previously mentioned with every involved actor. This to make sure that all actors involved in the implementation of the IT service continuity plan and during a recovery phase know what they are responsible for and what they have to do.

The following is an outline of the envisioned next steps underpinning ITSM's approach to addressing the above mentioned aspects and implementation of the IT service continuity plan.

DRP Organisation

A key issue to be addressed is to clearly define the responsibility perimeter of the involved actors and the components in scope. Identification of roles and responsibilities involved in the ITSM disaster recovery planning, crisis management process and assignment of responsibilities must reflect the organisational complexity and take into account the involvement of the various actors being DIGIT and CCN/TC. Functional units are part of different hierarchies within different service provider organisations; therefore this will require the involvement and commitment of DIGIT and CCN/TC management in order to establish the appropriate DRP matrix organisation.

Service Chain

It is important that in a large and complex environment where multiple service providers, service assets and resources combined deliver business services, not only the assets and resources on a physical and logical level are part of the DRP but the relations between them as well. These relationships should be translated into chains of services and dependencies which are represented in a hierarchical model of service assets, systems, applications, contracts, business services and the end users (customers).

It is necessary to perform a detailed asset impact analysis and dependency mapping exercise to map all inter dependencies between the applications, systems and the infrastructure across organisational boundaries. The analysis will help to identify, classify and prioritise the recovery of critical service assets (systems, applications, services, etc.) and highlight any major dependencies across organisational boundaries which can cause a risk in the recovery of assets and services during a crisis. The results of this step will assist in establishing the critical path, which represents those systems and components that must receive the highest priority during recovery. These recovery priorities should be considered simultaneously to determine what processing sequence should be followed across organisation boundaries so that activities that fall directly on the critical path receive the highest priority.

CCN/CSI is an integral part of the end-to-end business services. The recovery strategy for those systems under the responsibility of CCN/TC located at DIGIT and the ITSM premises should be based on the agreed business requirements and in line with the BCP/DRP strategy of ITSM and DIGIT. Although the CCN/CSI DRP does use application classification codes developed by the Commission, during our analysis we were unable to confirm if the DRP contains recovery time objectives that support the recovery of services within the maximum tolerated unavailability defined by the

application classification codes. Aligning the plans will ensure a cohesive CCN/TC recovery plan that supports the agreed business recovery objectives established in this document. This will ensure that the CCN/CSI assets can be recovered in line with the ITSM and DIGIT disaster recovery plans.

Application Classification

All service providers should use and apply one uniform application classification model to determine the appropriate measures required to satisfy the business requirements. A uniform classification will enable a more common and streamlined approach enabling all parties to align their plans with each other resulting in a cohesive set of recovery activities that contribute to achieving the established recovery objectives.

Recovery Time Objectives

The use of recovery time objectives and application of standards applicable to DG TAXUD Commission IT Services should be embedded into the provider organisations to enable the uniform application of these objectives and a streamlined approach across organisational silos. Current RTO's are most likely established in isolation and might not always align between providers, therefore impacting the effectiveness of DRP's. ITSM will conduct a GAP assessment and initiate the standardisation of business and IT RTO's during the next stage of the project.

Through the use of a standard application classification model and a standard business RTO model, in conjunction with the input received from the asset impact assessment and dependency mapping exercise, the service providers will be able to validate the feasibility of the business RTO's. Consequently, plans can be synchronised, recovery sequences adjusted and necessary technical or procedural changes applied as needed to meet the objectives.

Operating Level Agreements

The primary purpose of the Operating Level Agreement (OLA) is to ensure that a consistent level of service is provided by DIGIT and CCN/TC to ITSM in the context of the continuity plan. The OLA will define the roles and responsibilities that the service providers agree to follow during a disaster situation. It describes the responsibilities of each service provider towards the other, including the process and timeframe for recovery of their services. The objective of the OLA is to present a clear, concise and measurable description of the internal relationships between the service providers.

The purpose of the OLA's is very much to help ensure that the underpinning recovery activities that are performed by DIGIT and CCN/TC are clearly aligned to provide the intended objectives. Appropriate operating level agreements between all involved service providers and DG TAXUD must be established to ensure that relevant activities and performance levels in the context of the continuity plan and DRP are agreed and documented. An assessment of the existing OLA's through service level management must be conducted and possible GAP's in collaboration with continuity management

identified in order to establish the appropriate OLA's.

Service Level Objectives

Through close collaboration with service level management appropriate service level objectives applicable to a crisis situation must be established, agreed and documented. The final decision on what to use as service level objectives and the associated metrics must be defined as part of a working group meeting and/or workshop between the business sector leaders, business perspective managers, the ITSM contractor continuity and service level manager or designated backups. Subsequently, the objectives and agreements can be brought under change and configuration management control.

Working Group

A working group involving DIGIT, ITSM and CCN/TC representatives has to be implemented as a pre-requisite to the IT service continuity plan realisation. In particular, the working group will help in gathering the necessary information about the various environments and establishing the procedures that are required for the final ITSM DRP. This information mainly concerns the assets and dependency identification and valuation, the emergency incident assessment addressing potential disruptive threats such as, environmental disasters, organised and/or deliberate disruption, loss of external suppliers, equipment or system failure, serious information security incidents, and other emergency situations that impact the Commission IT services.

5.5 Planning

This section contains an overview of the stages and activities involved in the realisation of the proposed IT service continuity plan. It sets out the envisioned deployment and integration of the continuity plan and the DRP as described within this document and the recommendations included in it. The proposed stages are indicative and remain to be worked out into a proper project plan. All days are defined as working days.

Stage	Description of activities	Timing
DR solution[5] concept design and approval	Business requirements acceptance workshop with sector leaders and business perspective managers Proposal ITSM DR infrastructure solution concept Develop budget for ITSM DR solution concept including risk reduction measures Present options plus costs and obtain approval	T0[6]+30days

[5] Applicable to the ITSM delivered services only.

[6] T0 is the time at which this plan is formally accepted by TAXUD and the required approvals obtained to commence with the implementation as recommended in this section.

Stage	Description of activities	Timing
Project initiation and start-up	Form the project team and the project board Kick off meeting Planning workshops Define and agree scope and deliverables Write project initiation document and detailed project plan Workshops asset impact analysis and dependency mapping with DIGIT, CCN/TC and ITSM RTO feasibility and validation workshops with DIGIT, CCN/TC and ITSM Workshops recovery of applications with DIGIT CCN/TC and ITSM Workshops OLA, GAP assessment and requirements definition with DG TAXUD, DIGIT, CCN/TC and ITSM Workshop SLO's with DG TAXUD, ITSM, DIGIT and CCN/TC	T0+70days

Stage	Description of activities	Timing
Procurement[7]	Ordering and delivery of hardware Ordering and delivery of software and licenses Ordering and delivery of additional network circuits Ordering and delivery of additional backup tapes Order off-site storage service Ordering of third party services Ordering and delivery of equipment racks Ordering and delivery of cabling	T0+90days

Stage	Description of activities	Timing
Establish DRP organisation	Workshops DRP organisation with DGIT, CCN/TC, DG TAXUD and ITSM - Crisis management team	T0+90days

[7] Applies to the ITSM delivered services only

Stage	Description of activities	Timing
	- Coordination team - Recovery team - Roles and responsibilities - Invocation - Status identification and damage assessment - Team mobilisation DRP organisation approved (milestone)	

Stage	Description of activities	Timing
Infrastructure Solution Design[8]	**<u>Functional design</u>** EMC Storage Area Network Local Area Network Internet router failover Internet circuit Server systems Data synchronisation Security Functional specifications approved **<u>Technical design</u>** EMC Storage Area Network Local Area Network Internet Router failover Internet circuit Server systems Security Technical specifications approved (milestone)	T0+120days

Stage	Description of activities	Timing
Define, develop and document ITSCM procedures	**<u>Disaster recovery procedures</u>** Recovery of IT systems Recovery of telecommunication systems	T0+160days

[8] Applicable to the ITSM hosted infrastructure only.

Stage	Description of activities	Timing
	Recovery of software components Recovery of applications Recovery of data and volume groups Recovery of media Recovery of documentation Recovery of third party services Recovery of service desk operations **Other DRP procedures and asset documentation** Status identification and damage assessment Team mobilisation Staff call tree Information dissemination Specific recovery plan Progress monitoring and reporting Event logging form and procedure Hand over to operations Application list System list Hardware components Software components Third party services DRRT contact list	

Stage	Description of activities	Timing
Implement[9] stand-by DR arrangements and approved risk reduction measures	Prepare and equip stand-by site Install and configure computing hardware Install and configure computing software Install and configure applications Install and configure risk reduction measures Component testing System testing	T0[10]+175days

[9] Applies to the ITSM delivered services only. Planning for services delivered by other service providers remains their responsibility.

	Fine tuning Technical acceptance testing	

Stage	Description of activities	Timing
Education and awareness program[11]	Establish awareness program Launch awareness campaign Establish objectives and scope of training program Define training team Develop training materials Develop training schedule Train crisis management team Train coordination team Train recovery team	T0+180days

Stage	Description of activities	Timing
Develop and execute DR test plan (DLV.8.2.3.1.4.1[12])	This can be considered out of the test plan covered by the RfE nr 166. Determine objectives and scope of tests Establish test organisation Specify test scenarios Establish requirements for the test environment Develop test scripts Develop test quality control and monitoring process Finalise test plan and schedule Submit DR test plan to TAXUD for approval Submit DR test plan to CAB for approval Perform DR test Evaluate and submit DR test report including CSI recommendations	T0+150days

[10] T0 is herewith defined as the time of purchase date or purchase order submission

[11] Applies to the ITSM organisation only.

[12] This deliverable remains to be ordered by DG TAXUD and is not part of this plan by default.