OWNER:	ISSUE DATE:	VERSION:
DG TAXUD	22/06/2010	1.30

TAXATION AND CUSTOMS UNION DG
ITSM

SUBJECT:

IT Service Continuity Plan for Trans-European IT Services

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

FRAMEWORK CONTRACT # TAXUD/2007/CC/088

SPECIFIC CONTRACT 06

Document History

Edi.	Rev.	Date	Description	Action (*)	Pages
0	01	14/01/2009	Master document created	I	All
0	02	15/01/2009	Implementation of QC comments	I	All
0	10	15/01/2009	Sent for review to DG Taxation and Customs Union (SfR)	I	All
1	00	09/03/2009	Implementation of SfR meeting decisions. Sent for SfA	I	As req.
1	01	13/04/2010	Evolutive maintenance submitted to QC	I/R	As req.
1	02	14/04/2010	Implementation of QC comments	I/R	As req.

1	10	15/04/2010	Evolutive maintenance sent for review to DG Taxation and Customs Union (SfR) Update applications in scope of the TES and last mission reports on BCP/DRP in MSA until 31/12/2009	I,R	As req.
1	20	25/05/2010	Implementation of meeting decisions. Sent for Acceptance	I,R	As req.
1	30	22/06/2010	Submitted for re-acceptance. Implementation of meeting decisions.	I,R	As req.

(*) Action: I = Insert R = Replace

Table of Contents

Table of Tables

Table of Figures

1. Introduction

This document represents the formal Deliverable DLV.8.2.3.2.2 “IT Service Continuity Plan for Trans-European IT Services ” identified in Specific Contract SC06 to Framework Contract TAXUD/2007/CC/C088, Work Package WP.8.2.3.2.

1.1 Purpose of the document

The current IT Service Continuity Plan is a forward looking plan aimed at improving the overall TES IT Service continuity capabilities of the Member States to ensure that existing and future levels of IT Service continuity can be provided as agreed with the business. It specifies requirements for setting up and managing an effective IT Service continuity plan for trans-European systems.

The Commission steers the process to achieve agreements for the administrative cooperation by means of information technology. This involves standards, procedures, tools, technology and infrastructure. Currently, several IT Service continuity aspects have been agreed between National Administrations and the Commission for handling interruptions in the continuity of services. These are either addressed through service level agreements or specifications and are included as reference documents in section 1.8.1. This document is an extension to those agreements and concerns managing the ability of a Member State to continue to provide a pre-determined and agreed level of IT Service to support the minimum business requirements for trans-European systems following a major interruption or catastrophic event.

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

In order to achieve the goal mentioned above and taken into account the inter-dependent nature of trans-European systems, a set of standard requirements and rules should be defined and implemented by the Commission and Member States. A common and harmonised approach in the establishment of IT Service continuity requirements must be adopted. Additionally, there is a need for the minimum business requirements to be defined to a level of detail and agreed in order for Member States to develop appropriate disaster recovery plans and implement contingency measures.

This IT Service continuity plan (ITSCP) is the basis for defining and documenting those requirements in a harmonised and standardised manner and encompasses different IT Service continuity aspects that should be addressed by each Member State. It is a living document that will progressively change over time to reflect latest developments, agreements and progress being made in the improvement of Member State capabilities as it pertains to this ITSCP. It provides the structure required to evolve to a more mature plan in the future, some of the sections are already completed whereas others include

recommendations for completion at a later stage. Several recommended initiatives for improving this plan and a high level status of available BCP/DRP plans of the Member States are included as well

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 technical and service facilities 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);
5. Increase Business and Customer confidence as it is part of the Vision and Strategy of DG TAXUD.

1.2 Target Audience

The intended audience for this document is:

- the National Project Managers (NPM);
- the National Operations teams;
- Member State representatives and ITSM Business Monitoring Managers;
- DG TAXUD Sector leaders;
- Members of the Central Project Teams (CPT);
- ITSM Service Level Manager;
- CCN Contractor.

1.3 Scope

IT Service Continuity Management considers all aspects of the IT Infrastructure, the business and the supporting organisation, which may affect continuity, including, policy, people, process effectiveness, procedures and tools to ensure that the level of continuity delivered in all services matches the current and future agreed business needs. The scope includes all National domain components under the administrative responsibility of the Member States and applies to force majeure situations only. All Common domain components are covered by the IT Service continuity plan of the Commission.

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.

While the present document represents the first one of a list of annual reviews, as agreed with DG TAXUD, it mainly focuses on the existence of IT Service continuity capabilities and the initiatives to be undertaken to structurally improve these capabilities. The second main aim of the present document is also to establish a basis for conducting a more detailed and objective driven inventory of the IT Service continuity capabilities of the Member States in order to assist with the development of appropriate plans for all Member States with the goal to identify structural shortcomings and propose plans for improving capabilities where required.

This plan covers the services/applications for the following business threads (part of TES):

- Customs;
- Excise;
- Taxation.

The following scope statements apply to the applications and systems belonging to the various business threads:

1. All DDS applications are accessed through the DDS Portal, which is maintained by DG TAXUD and therefore part of the IT Service continuity plan for Commission IT Services and not of the present document;
2. Only production applications which are Nationally Operated are in the scope of the IT Service Continuity Plan for TES;
3. The Conformance Test environments, being hosted and operated by DG TAXUD, are out of the scope of this plan;
4. Testing applications like TTA, STTA, TA, etc, being all tools developed and operated by DG TAXUD, are not covered by the present plan;
5. Applications which are already foreseen but for which their entry in production is forecasted after 31/12/2009 are not covered by the scope of this document. Further updates of the TES IT Service continuity plan will include them in the scope.

1.4 Maintenance

As this document is based on a snapshot of the situation at a certain point in time it is necessary to have a maintenance process in place in order to keep this document up-to-date. This collection of information covering the status of the Member States was

stopped December 2009. The continuity plan needs to be revised periodically[1]. The plan will be revised through the annual review mechanism, at dates to be agreed with DG TAXUD within every Specific Contract (DLV.8.2.3.2.2 evolutive version of the IT Service Continuity Plan for the trans-European IT services).

1.5 Assumptions and Constraints

It is assumed that the reader of this IT Service Continuity Plan has a basic understanding of the IT Service Continuity Management process and the ITIL framework for Service Management.

The next version of the continuity plan will have to take into account the following documents (for continuity targets, objectives and metrics):

- SLA(s) per business thread and/or application[2];
- OLA(s) (if applicable);
- Underpinning contracts covering standby arrangements with third parties.

No information was available for this evolutive maintenance version.

The improvement actions covered in this plan are primarily related to improving the capabilities of the continuity management process itself, rather than the continuity capabilities of the underlying ICT infrastructure (including the applications).

[1] Periodic revision of the continuity plan is described in the FQP which is available on Knowledge Tree within ITSM. A copy of the reference documents can be requested from DG TAXUD if access to Knowledge Tree within ITSM is not possible

[2] Outcome of the one-off DLV.8.2.1.2.1 Harmonised & converged Service Catalogues & SLAs, per customer/user community across all taken over business threads and ITSM thread.

1.6 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	**Trans-European System Description and Scope** Presents the scope of TES and the plan listing the applications scope.
Chapter 3	**TES BCP/DRP Status Assessment** Provides an overview of the status of existing BCP/DRP plans within the Member States.
Chapter 4	**Requirements and Strategy** Lists the business requirements and the recovery strategy applicable to the applications and services in scope of this document.
Chapter 5	**ITSCM Improvement Plan** Documents the recommendations, next steps and planning aspects associated with the realisation of the recommended improvement initiatives.
Annex A	**Status Overview Customs** Provides a status overview and extracted information from mission reports relevant to the status of BCP/DRP plans within the Member States.
Annex B	**Assessment Questionnaire** Presents a list with questions pertaining to the required assessment described in this document. This includes definitions relevant to the questions.
Annex C	**BIA Matrix** Presents a sample matrix that can be used to conduct an initial business impact analysis.
Annex D	**Status Overview Taxation** Provides an overview describing the status of BCP/DRP plans within the Member States collected from the questionnaire.

Table 1-1: Document structure

1.7 Reference and Applicable Documents

1.7.1 Reference Documents

All ITSM documents are available on the ITSM Portal within ITSM.

Id	Reference	Title	Date	Version
RD1	ITS-IGLO-ITSM	ITSM Glossary	N/A	V1.11
RD2	TMP-REF-DRL	Disaster Recovery Plan (Life Cycle)	24/08/2006	V2.02-EN
RD3	TMP-GDL-DRP	Disaster Recovery Plan (Guide)	24/08/2006	V2.01-EN
RD4	TMP-TEM-DRP	DG TAXUD A3 - Disaster Recovery Plan (Template)	09/02/2006	V2.02-EN
RD5	ITS-IFQP-SC01-Framework Quality Plan	Framework Quality Plan	23/03/2010	V1.04
RD6	ITSM-DLV8.6.1.3.1-Technical Infrastructure Reference	TAXUD Technical Infrastructure Reference	13/10/2008	V0.11
RD7	TMP-FAC-DCS	Data process and system classification Fact Sheet	12/09/2006	V1.3-EN
RD8	TMP-REF-ITSCM	IT Service Continuity Management	05/02/2008	V1.50-EN
RD9	ITIL V3 Service Design	Service Design	2007	
RD10	ITS-ITOC-eCUST-TES-v3-1-1	Terms of Collaboration between the Central Project Team and the National Project Teams	07/04/2010	V3.1.1
RD11	ITS-ISLA-eCUST-TES-ACM	Service Level Agreement for Availability and Continuity of Customs Trans-European Systems between DG TAXUD and National Administrations	07/04/2010	V3.1.1
RD12	SCIT68 -SLA	Service Level Agreement (VAT related systems)	14/03/2008	V3.00
RD13		IT Service Continuity Plan for Trans-European IT Services - General template	09/03/2009	1.21

Id	Reference	Title	Date	Version
RD14	Annex I – Specifications for implementing Availability and Continuity in NCTS	Specifications for implementing availability and continuity in NCTS	16/06/2006	1.06-EN

Table 1-2: Reference documents

1.7.2 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

1.8 Terminology

1.8.1 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
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CCN	Common Communications Network
CCN/CSI	Common Communications Network/Common System Interface
CCN/TC	Common Communications Network/Technical Centre
CDA	Centrally Developed Application
CDTA	Centrally Developed Transit Application
Circa	Communication & Information Resource Center Administrator
CPT	Central Project Team

Abbreviation / Acronym	Description
CSIP	Continuous Service Improvement Program
DG TAXUD	Directorate-General for Taxation and Customs Union
DIGIT	Directorate–General for Informatics
DIGIT/DC	Directorate–General for Informatics/Data Centre
DRP	Disaster Recovery Plan
IT	Information Technology
ITSCM	IT Service Continuity Management (also shortened to Continuity Management in this document)
MTPU	Maximum tolerated period of unavailability
NAs	National Administrations
NDA	Nationally Developed Application
NPM	National Project Managers
NPT	National Project Team
OLA	Operating Level Agreement
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
SLO	Service Level Objective
TEMPO	Quality Management System of DG TAXUD IT (TAXUD Electronic Management of Projects On-line)
TES	Trans European System
ToC	Terms of Collaboration

Table 1-4: Abbreviations and acronyms

1.8.2 Definitions

The definitions below have been taken from the following sources:

- ITS-IFQP-SC01-Framework Quality Plan [RD5]
- ITS-ITOC-SLA-ACM [RD11]
- ITIL V3 Service Design [RD9]
- Wikipedia

Term	Definition
Activity	A set of actions designed to achieve a particular result.
Business Continuity Management	The Business Process is responsible for managing risks that could seriously affect the business. BCM safeguards the interests of key stakeholders, reputation, brand and value creating activities. The BCM Process involves reducing Risks to an acceptable level and planning for the recovery of business processes should a disruption to the business occur. BCM sets the objectives, scope, and requirements for IT Service Continuity Management.
Business Continuity Plan	A documented collection of procedures and information developed compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at an acceptable pre-defined level.
Business Impact Analysis	BIA is the activity in Business Continuity Management that identifies vital business functions and their dependencies. BIA defines the Recovery requirements for IT Services including Recovery Time Objectives, Recovery Point Objectives and minimum Service Level Targets for each IT Service.
Capability	The ability of an organisation, person, process, application, configuration item or IT service to carry out an activity as intended.
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.
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 incident management process.
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. Impact describes the measure of the business criticality of an incident. Impact is often based on the extent to which an incident leads to distortion of agreed or expected Service Levels.

Term	Definition
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.
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.
Maximum tolerated period of unavailability	Duration after which an organisation's viability will be irrevocably threatened if product and service delivery cannot be resumed.
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.
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 tolerated period of unavailability.
Unscheduled unavailability (alias "U")	Unscheduled unavailability is a sudden disruption (or a disruption planned less than 48 hours in advance) of one or more IT services or severe service degradation in terms of performance.
Scheduled Unavailability (alias "S")	A planned disruption of one or more national or central services.
JBoss architecture	The structure or structures of a JBoss program or computing system, which comprise software components, the externally visible properties of those components, and the relationships between them.

Table 1-5: List of definitions

2. Trans-European System Description and Scope

The present chapter explains the IT architecture and business organisation of IT systems under the scope of this document.

2.1 Introduction

A trans-European system is a set of collaborative business processes, services, applications and infrastructure distributed in National Administrations and at the European Commission, in order to perform a given business activity.

The portfolio of IT services provided by DG TAXUD is composed of a set of systems and applications. This portfolio is currently organised in four business threads as follows:

- **Customs TES and applications,** this thread includes:
    - The new Computerised Transit System (NCTS) and applications underpinning the NCTS which is expanded to Customs and in particular the Export Control System (ECS). NCTS and ECS are distributed trans-European systems with CCN as backbone. To this one has to bear in mind the future developments of further applications like the Import Control System (ICS) and Economic Operators System;
    - The Tariff oriented applications, Risk Information System, Activity Reporting Tool for the management of programmes and the Data Dissemination System on Europa. These applications run on the IT infrastructure of the Data Centre (DC) of DIGIT and the ITSM contractor and most of them are centralised trans-European systems relying on CCN for the secure connectivity with NAs;
- **Excise TES and applications**: The flagship of this thread is EMCS (currently under development) but there are a set of small- and medium-size systems already in operation (SEED, EWSE, MVS). The Excise systems are distributed trans-European systems with CCN at their core;
- **Taxation TES and applications**: the flagship of this thread is the VAT Information Exchange System (VIES) which is complemented with the VAT on e-Services (VoeS), VIES-on-the-Web, Taxes in Europe DataBase (TEDB), Taxation on Savings and e-Forms applications. VIES and Taxation on Savings are distributed trans-European systems, taking advantage of CCN. Both VoeS and e-Forms are distributed and centrally operated and deployed. VIES-on-the-Web and Taxes in Europe DataBase are currently hosted at the DIGIT/DC.

From an IT point of view, a trans-European system is a series of software components running in the National Administrations and/or at the European Commission and which

communicate with each other via a secure trans-European network, the Common Communication Network (CCN).

There are different architectures of trans-European systems, in certain cases National Administrations communicate directly to one another, in other cases they all communicate to a single central application. The principle of the TES is the following: all National Administrations, and the Commission connect to a trans-European Network for exchanging information (Information Exchange, IE) either with one another, either with a central application.

The trans-European systems developed and operated under DG TAXUD coordination concern Customs, Taxation or Excise business. For those TES that are developed and operated at DG TAXUD, the business process model is mainly oriented to the consolidation of information from National Administrations and broadcasting information to National Administrations and on business movement process. The sensitivity of the information transferred and the visibility of the operation imposes that different security aspects are considered during the complete lifecycle of the TES.

DG TAXUD offers a series of services to support the entire lifecycle of all trans-European systems, such as creation of specifications, testing, monitoring, statistics, Service Desk. These aspects are out of the scope of the present document.

2.2 CCN

The trans-European systems developed and operated under DG TAXUD coordination rely all on the Common Communication Network (CCN). The CCN allows a harmonised approach to the application development and operation, in compliance with the regulatory constraints of the European Commission in the context of data transmission.

As described by TEMPO, the CCN allows the coexistence of several application flow types meeting different needs of interoperability between National Administrations. The exchange channels are based on:

- The proprietary protocol (Common System Interface, CSI) meeting the need of interoperability between heterogeneous systems;
- The standard HTTP or HTTPS protocol used by services offered on the “CCN Intranet”;
- CCN Mail;
- SOAP.

The CCN, with its corresponding gateways defines the limits of the Common Domain.

2.3 TES Architecture Models

DG TAXUD business is oriented on two main architectural models of trans-European systems: Distributed and Centralised TES.

2.3.1 Distributed TES model

A Distributed TES has the main system functionality operated in the National Domain of each National Administration (distributed) and is under the responsibility of each National Administration. Users (NAs, National Offices, Traders) are able to exchange information directly with users and applications in other Member States/countries over the CCN by using the Nationally Developed Application (NDA). Distributed TES are developed and operated by the National Administrations. A typical distributed TES is shown in the following figure.

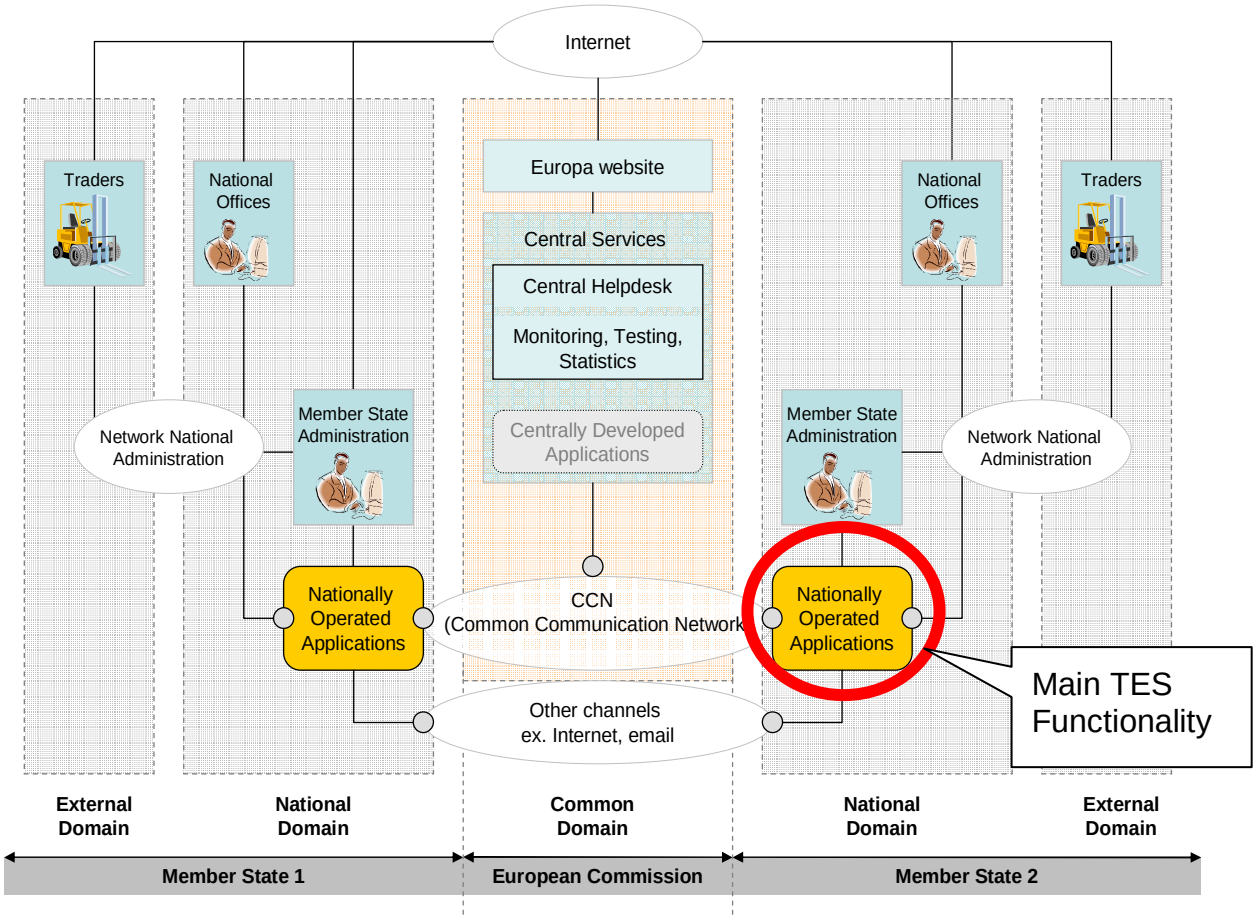

Figure 1: Typical Distributed TES[3]

[3] Source : TEMPO Methodology [RD13]

The three domains of responsibility are clearly separated: the Common Domain is managed by the Commission, whereas the National Domain falls under the responsibility of each National Administration. The Common Domain comprises the CCN, the Central Services, and the Centrally Developed Applications (CDA), which may implement some functionality of the TES.

All users in the National and External Domains (NAs, National Offices, Traders) access the Nationally Developed Applications through the National Administration Network.

NDAs implement the main part of the TES functionality. Users in one NA exchange information with users in another country interacting with their NDA, which transfers messages to other NDAs via the secure CCN. Depending on how the TES have been conceived, NDAs may exchange messages also via other channels than the CCN, such as the Internet, mainly as fallback.

2.3.2 Centralised TES

A Centralised TES has its main system functionality operated in the Common Domain (centrally) under the responsibility of the Commission. National Administrations are able to interact with and exchange information through the Centralised TES. The applications of the centralised TES are accessible to the National Administrations remotely.

As described by TEMPO, a typical Centralised TES is depicted in the following figure.

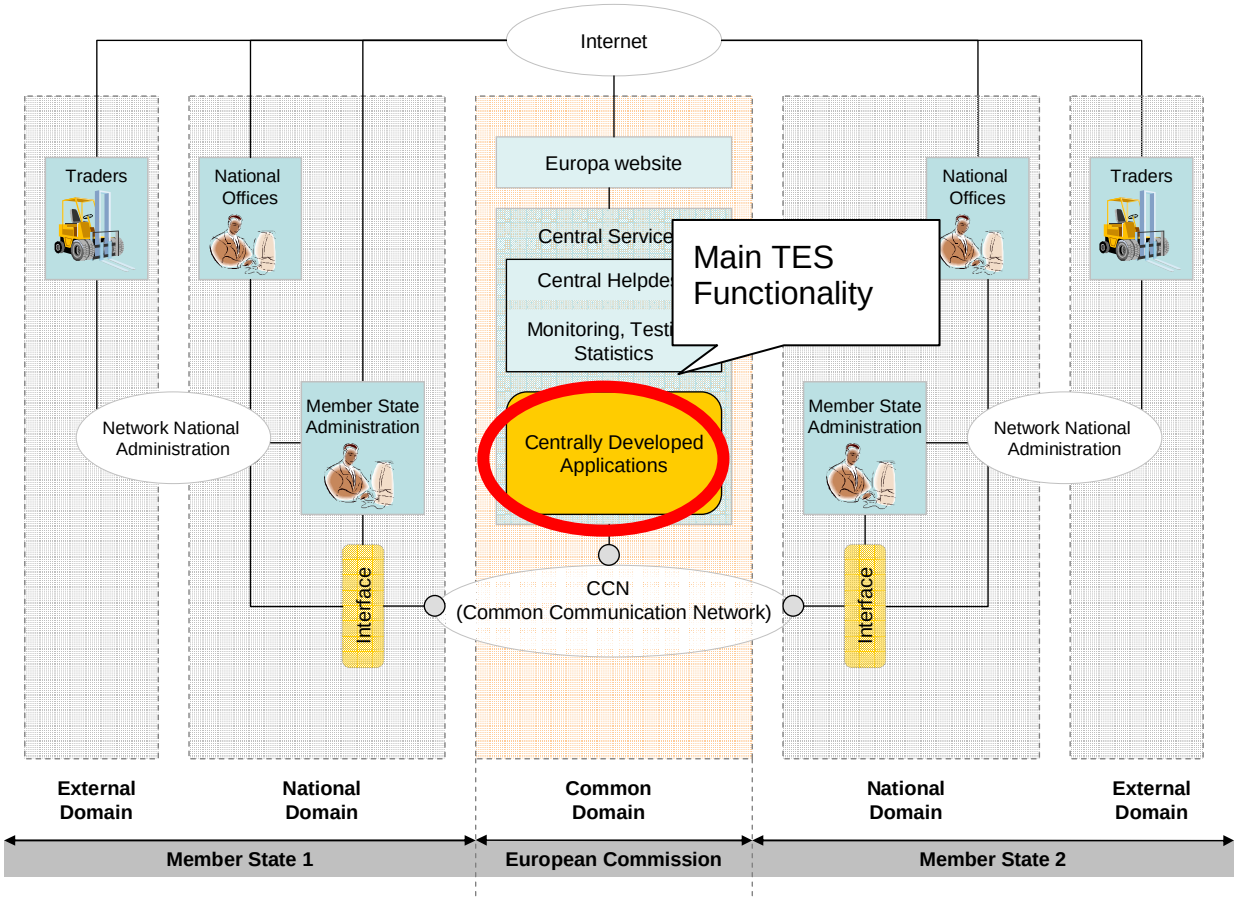

Figure 2: Typical Centralised TES[4]

The three domains of responsibility are clearly separated. The Common Domain is managed by the Commission whereas the National Domain and the External Domain fall under the responsibility of each National Administration. The Common Domain comprises the CCN, the Central Services and the Centrally Developed Applications (CDA), which implement the main functionality of the TES.

All users in the National Domain (NAs, National Offices) access the CDA and the Central Services through the National Administration Network via a client application (Interface), which mainly serves as a relay to the CCN.

Figure 2 also shows that users may access the CDA and the Central Services via other channels, such as the Internet. An example of a centralised TES is the Tariff Quota and Surveillance System (TQS).

[4] Source : TEMPO Methodology [RD13]

2.4 Mixed Architecture

In the case of Distributed TES, where the business is based on the communication between NAs, it may happen that some parts rely on Centralised TES (e.g. in NCTS, the list of Customs Office is maintained centrally). The distinction between Distributed and Centralised TES is mostly based on the business logic of the system but does not imply that there is a complete separation between both TES models (Centralised or Distributed).

2.5 TES Process Model

In addition to the architecture of the different TES, another classification can be performed based on the type of information that is exchanged in the trans-European systems. Two main types of TES can be identified:

- **Business Systems/applications**: where the messages (Information Exchange) exchanged between the different participant organisations reflect state changes of business event activities (*e.g.* the departure of a movement in the NCTS system);
- **Reference Systems/applications**: Where the messages exchanged are used to disseminate information created/owned by one author and shared with multiple possible readers in other National Administrations or in Data Centre (*e.g.* Taxes in Europe DataBase).

Table 2-1 provides a classification of different TES in development and/or operations under DG TAXUD responsibility based on the architectural model (Centralised/Distributed) and the process model (Reference/Business). This table highlights the independence between the process model of a TES and its architecture. The supporting applications (VIES Monitoring, CS/RD…) are all centralised and are omitted in Table 2-1.

	Centralised TES	Distributed TES
Reference	*Customs Business Thread :* DDS, EBTI TARIC (including commercial policies related applications): Suspensions CN, ISPP Unit values ECICS Transit/Export/Import/Economic Operators reference *Excise Business Thread :* Excise Registration Details (SEED) *Taxation Business Thread :* *TEDB, VIES on the WEB*	*Customs Business Thread* *Taxation Business Thread*
Business	*Customs Business Thread :* Tariff Quota Surveillance CRMS ART *Customs Business Thread :* Customs EOS	*Customs Business Thread:* NCTS, ECS, ICS *Excise Business Thread :* EMCS, EWSE,,SEED, MVS *Taxation Business Thread :* VoeS, Tax on Savings, VIES,e-Forms

Table 2-1: DG TAXUD trans-European systems [5]

2.6 Applications in Scope of the TES IT Service Continuity Plan

The applications in scope of the TES IT Service continuity plan are described in the following table.

Business Thread	Application
Customs	National Transit Applications, NTA
	National Economic Operational System, EOS
	National Import Control Applications, NICA
	National Export Control Applications, NECA

[5] Source : TEMPO Methodology [REF 13]

Business Thread	Application
Excise	SEED
	MVS
	EWSE
Taxation	VAT Information Exchange System
	VAT-on-e-Services
	Taxation on Savings
	e-Forms

Table 2-2: List of applications in scope of the TES IT Service continuity plan

3. TES BCP/DRP Status Assessment

3.1 Introduction

This section describes at a high level the status of some BCP/DRP related aspects applicable to the National Administrations. The presented overview does not comprise a detailed assessment nor does it provide an extensive analysis of every aspect of IT Service continuity management or assess the maturity of existing plans and processes in the context of the National Administrations. This goes beyond the scope of this document.

The results of the status assessment are based on the responses received and reviewed, and additional interviews conducted with several Member State contacts. Interpretation of the information in this section might not always align to reality due to the following:

- Missing relevant information and/or informal information not processed within this document;
- Different interpretation of content due to inconsistent use and application of terminology and lack of detailed information;
- BCP and DRP term used interchangeably, no distinction made between BCP and DRP in the questions used as part of the inventory.

3.2 Status Assessment Results

The result of the assessment is an overview which is based on a preliminary inventory that was done through an e-mail sent to all Member States on 21/08/2008 in combination with an analysis of the mission reports since that date.. The objective of the e-mail was to obtain some high level information about the status of BCP/DRP plans within the Member States and to conduct an initial status assessment. The following questions, in agreement with DG TAXUD, were e-mailed to all National Administration contacts:

1. Does a BCP/DRP exist?
2. Has it been communicated?
3. Is it maintained?
4. Have tests been done?
5. What is the scope
6. Can you provide a copy of the BCP/DRP?

Although the information obtained does provide a high level view of the status within some Member States it is not sufficient and not detailed enough to conduct a proper assessment at this stage.

Based on the results and assessment of the information gathering exercise, Member States can be grouped into five main groups, being:

1. There is no existence of a business continuity or disaster recovery plan at this stage;
2. A partial business continuity plan does exist however a comprehensive disaster recovery plan is missing;
3. Information is still outstanding and follow up is required;
4. A business continuity project has been started and is ongoing at this stage;
5. An operational ready to use BCP/DRP is in place and tests are being conducted.

The above indicates that the status within each Member State is very diverse and that the approach therefore in obtaining additional information to assess the status should be adapted accordingly.

More detailed and specific information covering each Member State can be found in Annex A for Customs and Annex D for Taxation.

The inventory and assessment results should provide an objective and sufficiently detailed perspective of the current plans and process state for TES and enable possible gaps between the capabilities of the Member States and the requirements (see chapter 4) to be identified and addressed. Obtaining this objective perspective and understanding of the status based on the six inventory questions is not possible. The information is not sufficient nor structured enough to conduct a proper assessment of the status.

3.3 Conclusions

As mentioned in the previous section, there is a need to conduct a more thorough assessment in order to obtain a comprehensive and objective view of the status. Only then will the ITSM contractor be in the position to identify areas for improvement that contribute to achieving the objectives of the IT Service Continuity Management process.

Assessments can be targeted broadly or focused specifically where known problems exist, this implies that there are multiple scope levels that must be addressed prior to engaging on the assessment. Determining the assessment's scope and objectives is one of the key items to be addressed prior to engaging further with gathering information. The scope should be based on the assessment's objectives and the expected future use.

As long as the scope and objectives of the assessment is not based on specific and agreed requirements, and the status per Member State not determined based on those objectives, there is a risk of creating a situation that negatively impacts the ability of DG TAXUD and the Member States to structurally drive the improvement of the IT Service continuity capabilities. This results in the following effects:

- A gap or overlap between the Member State plans and this plan;
- Lack of insight into areas which have room for improvement;
- Variances in process maturity levels hence making continuity plans less efficient;
- Difficulties determining the variance between business requirements and current capabilities.

To avoid such situation and creating the conditions of an effective development and maintenance of this plan, the use of a more pragmatic assessment based on specific objectives in the form of a gap analysis must be conducted. The gap analysis should be part of the CSIP and enables DG TAXUD and the Member States to compare where they are currently and where they need to be in the future. This provides the organisation with insight to areas which have room for improvement and can be used to determine the gap between "the Vision & Strategy, the current state and the future state" and enables a roadmap to be developed. Subsequently, the "future state" can be formalised within the ToC for Availability and Continuity of all trans-European systems in scope of this plan. Section 5 contains information on the recommended approach for a more thorough and objective based gap analysis.

4. Requirements and Strategy

This section describes various aspects relevant to the requirements and strategy of the TES IT Service continuity plan. It aims to describe and address the requirements from a business perspective.

4.1 Requirements

4.1.1 Business Impact Analysis

The BIA forms the corner stone of the IT Service continuity planning process. As part of the assessment we were unable to confirm the existence of a BIA and the results of the analysis. It is therefore a priority in the list of items to be addressed and the results should be part of the next iteration of this plan.

The below table lists the elements part of the BIA that, at a minimum, need to be part of the IT Service continuity plan.

#	Description
1	Impact of the loss of a service in terms of revenue, reputation, operations and strategy
2	Maximum tolerated unavailability times
3	Standard time-bands for measuring periods
4	IT asset mapping and classification
5	Recovery priorities (none IT assets)
6	Critical business hours and periods

Table 4-1: BIA elements in scope

4.1.2 Availability Requirements and Classification[6]

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. These classification levels have been adapted to reflect the context of this plan and do not necessarily match the exact definition of [RD7]

- *MODERATE: This classification shall apply to information or information systems the loss of whose integrity or availability might threaten the internal working of the Member State;*

[6] The classification levels used have been adapted to fit the context of this plan and do not fully align to those defined by 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 Member State with regard to other Institutions, Member States, the Commission 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 Member State, to other Institutions, to the Commission or to other parties.*

The table below provides the list of the applications currently in scope of this document including their availability requirements specified in continuous hours and corresponding classification based on ITSM contractor's experience, the classification levels and knowledge of the business. These are used merely as guidelines and shall be confirmed as soon as the BIA has been completed. For each of the applications the following indications are provided:

- Availability requirements expressed in maximum tolerated 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 remain to be formally agreed by the sector leaders in cooperation with the ITSM business perspective manager(s) during the next phase.

Application/ Service name	Availability Requirements (Maximum tolerated period of unavailability)	Availability Classification
National Transit Applications, NTA	Unavailability will have a critical impact on Member States and citizens. The tolerated unavailability of the system is judged to be between 3,5 and 48 hours.	Critical
National Economic Operational System, EOS	Unavailability will have a critical impact on Member States and citizens. The tolerated unavailability of the system is judged to be between 3,5 and 48 hours.	Critical
National Import Control Applications, NICA	Unavailability will have a critical impact on Member States and citizens. The tolerated unavailability of the system is judged to be between 3,5 and 48 hours.	Critical
National Export	Unavailability will have a critical impact on Member States and citizens. The tolerated unavailability of the	Critical

Application/ Service name	Availability Requirements (Maximum tolerated period of unavailability)	Availability Classification
Control Applications, NECA	system is judged to be between 3,5 and 48 hours.	
ICS	Unavailability will have a critical impact on Member States and citizens. The tolerated unavailability of the system is judged to be between 3,5 and 48 hours.	Critical
MVS	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
SEED	Unavailability of the system will have an impact on critical processes and the Member States. The maximum tolerated period of unavailability of the system is judged to be between 3,5 and 48 hours.	Critical
EWSE	Unavailability will have impact on Member States. The maximum tolerated period of unavailability of the system is judged to be above 48 hours.	Moderate
VAT Information Exchange System	Unavailability of the system will have an impact on Member States and the citizens. The maximum tolerated period of unavailability of the system is judged to be above 48 hours.	Moderate
VAT-on-e-Services	Unavailability will have impact on Member States and the citizens. The maximum tolerated period of unavailability of the system is judged to be above 48 hours.	Moderate
Taxation on Savings	Unavailability will have impact on Member States and the citizens. The maximum tolerated period of unavailability of the system is judged to be no above 48 hours.	Moderate
e-Forms	Unavailability will have impact on Member States. The maximum tolerated period of unavailability of the system is judged to be above 48 hours.	Moderate

Table 4-2: Continuity requirements of applications

4.1.3 Risk Assessment

The risk analysis can be approached from different perspectives and can be a daunting task if not scoped properly considering the scale of this trans-European project. It is important to consider the context of this analysis in order to propose a method that meets the objectives of the process. Where traditional risk analysis methods focus on

threats, vulnerabilities and control measures, this recommended risk analysis focuses on process capabilities within the Member States.

Conducting a detailed risk analysis for all Member States requires at a minimum a mission of three days per member state to be initiated. This is resource intensive, time consuming and might overlap with risk management activities and plans of the Member States. The recommendation therefore is to use an alternative method which identifies at a high level the risks per Member State which directly relate to this plan and the process capabilities.

Through the use of a risk assessment questionnaire information should be obtained which can subsequently be analysed and an assessment conducted on the maturity and/or risks applicable to specific target areas. This risk assessment should not focus on traditional risk assessment and management aspects but focus solely on those aspects relevant to achieving the objectives of the plan. Subsequently, the assessment will enable appropriate risk response measures to be recommended and implemented in order to manage the risks.

4.2 Strategy

4.2.1 Business Recovery Time Objectives

This is the target set for recovering the applications and services from a business perspective to allow business processes to be resumed within the maximum tolerated period of unavailability. Business recovery time objectives are driven by the business impact analysis BIA.

The below suggested business RTO's are within the limits imposed by the 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 RTO 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
Customs	National Transit Applications, NTA	Tier 2
	National Economic Operational System, EOS	Tier 2
	National Import Control Applications, NICA	Tier 2

Business thread/Service	Application/ Service name	Recovery Time Objective
	National Export Control Applications, NECA	Tier 2
Excise	MVS	Tier 3
	SEED	Tier 2
	EWSE	Tier 3
Taxation	VAT Information Exchange System	Tier 3
	VAT-on-e-Services	Tier 3
	Taxation on Savings	Tier 3
	e-Forms	Tier 3

Table 4-3: Business recovery time objectives

4.2.2 Recovery Point Objectives

SLAs will be analysed aswell as RPO's defined for the applications in scope of this plan. Existing RPO's are from a business point of view. The following RPO tiers should be defined as follows:

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
Customs	National Transit Applications, NTA	Tier 2
	National Economic Operational System, EOS	Tier 1
	National Import Control Applications, NICA	Tier 1
	National Export Control Applications, NECA	Tier 1
Excise	MVS	Tier 2
	SEED	Tier 1
	EWSE	Tier 2
Taxation	VAT Information Exchange System	Tier 2
	VAT-on-e-Services	Tier 2
	Taxation of Savings	Tier 2
	e-Forms	Tier 2

Table 4-4: Recovery point objectives

4.2.3 Service Level Objectives

The Service Level Objectives (SLO) during a disaster situation should be described in this plan and formalised through service level management. 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.

There are currently no service level objectives defined, these remain to be developed and agreed. Subsequently, these should be referred to in the SLA for availability and continuity management.

4.2.4 Recovery Strategy[7]

Different services within the organisation require different built-in resilience and different recovery options. Whatever 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 will describe the various recovery options available including a matrix with the selected options per application and services in scope of this plan. The selected options are based on the availability requirements of the applications as defined in section 4.1.2 and the business recovery time objectives in section 4.1.3**.** These recovery options have been taken from the ITIL framework [RD9] and slightly adjusted to fit the context.

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.

[7] Time dependencies that influence an outage impact and subsequently the recovery priority or recovery strategy of systems have not been taken into account.

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 centre 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)
National Transit Applications, NTA			X		
National Economic Operational System, EOS			X		
National Import Control Applications, NICA			X		

Application/ Service	Manual Recovery	Gradual Recovery (>48hrs)	Intermediate Recovery (3,5hrs-48hrs)	Fast Recovery (<3,5hrs)	Immediate Recovery (real-time)
National Economic Operational System, EOS			X		
National Export Control Applications, NECA			X		
ICS			X		
MVS			X		
SEED			X		
EWSE		X			
VAT Information Exchange System			X		
VAT-on-e-Services		X			
Taxation on Savings		X			
e-Forms	X				

Table 4-5: Matrix with recommended recovery strategies

5. ITSCM Improvement Plan

5.1 Introduction

The realisation of the TES continuity plan will not happen overnight and needs an approach and guidelines that facilitates incremental changes to be realised until the goals of the plan are achieved. The extensive details involved in this pan-European initiative demands a systematic and incremental approach. The current status of the TES IT Service continuity plan gives a solid foundation for further development and improvement of capabilities. It presents a thorough coverage of aspects that need to be addressed in order to realise the further development and implementation of the plan on a pan-European scale.

This section structures and aggregates a range of initiatives which facilitate the realisation of the plan and implementation of opportunities to improve the overall effectiveness of IT Service continuity management capabilities within the organisation. Through the proposed initiatives, baselines are established in order to facilitate comparison (An important beginning point for highlighting improvement is to establish baselines as markers or starting points for later comparison) and a gap is produced.

The initiatives support the concept of continuous improvement as described within the FQP [RD5] and provide key input for the overall Continuous Service Improvement Programme (CSIP). In subsequent iterations of the plan, the initial baseline will be updated; it will also include the results of the proposed initiatives and provide additional considerations, recommendations and guidelines to commence with evolving the plan to the next level.

5.2 Plan Evolution

As the IT Service Continuity Management process matures the plan should evolve to cover the following:

1. Agreed standards, norms and methods; this should encompass training and testing standards to facilitate uniformity;
2. Risk analysis and assessment results per Member State including proposed risk reduction measures;
3. Agreed business requirements, through a BIA, and formalised recovery strategy's; the first step in establishing the bases for the plans;
4. Review/Audit on a regular basis the actual levels of capabilities, from a holistic standpoint including processes, people, organisation, knowledge, and standby arrangement versus agreed/required levels of capabilities;
5. Activities being progressed to address shortcomings in continuity management capabilities for IT services and applications in scope;

6. A forward looking schedule for planned disaster recovery tests and training plans; a standard test program and recurring schedule should be agreed amongst all Member States in order to avoid possible conflicts enable the plans to be synchronised.

The recommended initiatives in the following section focus, to a certain extent, on items one, two, three and four.

5.3 Recommended Initiatives

5.3.1 Business Impact Analysis

A BIA is the first logical step and a priority in the further development of the TES IT Service continuity plan and provides the business rationale for continuity and disaster recovery planning. It will help validate if current capabilities in terms of organisation, technology, processes and procedures align to business needs and are sufficient to recover trans-European systems from a disastrous event.

Information produced from the BIA serves as input for the following stages, therefore it is recommended to start, as a priority, a preliminary BIA assessment that can as needed, evolve to a more mature assessment over time. The following is a recommended pragmatic approach to produce the initial BIA. It covers the main requirements of a BIA and establishes a sound basis for further development.

1. Business impacts are identified based on a worst-case scenario that assumes that the physical infrastructure supporting each respective application has been destroyed and all records, equipment, etc. are not accessible. Impacts are rated per impact type on a scale of 0-5. See Annex C for the recommended sample BIA matrix including impact types and impact levels. The impact value is an indication of the severity of the impact to the business that would result if the business units were unable to function as a result of the unavailability of the system and is used to establish the maximum tolerated down time.

2. It is necessary to establish time bands when, during an emergency, optimal business services could become unavailable. These time-bands are then applied to each key business application and an assessment made of the financial, operational, political and strategic impact and damage level.

3. The used classifications of the applications and services part of the scope of this plan are then confirmed and consensus reached with the business sector leaders and the Member State representatives. The classification levels used are those extracted from [RD7] and indicate the extent of criticality of the applications and services.

5.3.2 Risk Analysis

Risks introduced as a result of the process capabilities within the Member States should be identified, assessed and classified accordingly. The purpose of this is to enable

realistic and practical judgements to be made on measures to take to increase the process capabilities of the Member States in order to reduce the identified risks.

This section suggests a list with target assessment areas which are critical to the ability of a Member State to meet the process objectives. The following aspects and sub-aspects are the target areas of the risk assessment that should be scoped and subsequently assessed. These target areas and the overall approach remains to be agreed between the ITSM contractor, DG TAXUD and the Member States.

Category	Aspect	Sub-aspect
Requirements and Strategy	Risk Analysis	System characterisation
		Threat identification
		Vulnerability identification
		Control analysis
		Likelihood determination
		Risk determination
		Control recommendations
		Results documentation and management acceptance of the residual risks
Implementation	Disaster recovery plan	System recovery time objectives
		Damage and impact levels
		Recovery priorities and time frames
		Organisation
		Activation parameters
		Invocation authorisation
		Incident response team mobilisation
		Damage assessment
		Preparation of specific DR plan
		Progress monitoring and reporting
		Communication
		Event logging
		Hand over to normal operation
		Detailed recovery procedures
		Stand-by arrangements
Operational Management	Training plan	Organisation
		Training requirements
		Training materials
		Training schedule
		Communication on training
Operational Management	Disaster recovery test plan	Objectives and scope of tests
		Test environment

Category	Aspect	Sub-aspect
		Test data
		Organisation
		Test control and monitoring process
		Testing team training
		Test schedules
		Test result assessment and review cycle

Table 5-1: List of risk analysis target areas

The approach of the risk analysis depends on the final scope and the assigned priorities per aspect and sub-aspect. This must be discussed and agreed prior to starting the analysis. One possible approach for example is to divide all aspects into multiple assessment blocks and phases that can be initiated throughout a period of for example two years. Considering the scale of the initiative, it is recommended to develop an approach that enables the assessment to take place over a longer period managed through the CSIP and align the priorities to the overall planning of this continuity plan.

5.3.3 Recovery Objectives & Strategy

Formalising the business recovery objectives is the next logical step after the BIA and considered the next priority for the next iteration of the plan. The outage impact(s) and maximum tolerated unavailability times defined as part of the BIA enable business recovery time objectives for each IT Service and/or application to be agreed and formalised on a pan-European level. Subsequently, recovery strategies can be confirmed and agreed with the business to meet the agreed recovery objectives. The strategy must also address recovering information system critical components within a priority, as established by their individual recovery time objectives.

The results of this step will assist Member States in establishing and/or comparing system RTOs and RPOs, and establish the critical recovery path, which represents those systems that must receive the highest priority during recovery. The RPO in conjunction with the system recovery time objective (RTO) is the basis on which Member States can develop data protection strategies.

5.3.4 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 table below presents an overview with elements for which the scope must be formalised as part of the evolution of the continuity plan.

#	Description
1	Minimum hours of service required.
2	Critical periods of service, peaks, month-end, deadline processing, and so on.
3	Less critical periods of service where downtime is more tolerated.
4	Scheduled unavailability periods for planned maintenance and upgrades.
5	Capacity and performance targets.
6	Availability targets.
7	Recovery time and recovery point objectives.
8	Maximum allowed time for operating at the agreed DR service levels or objectives.

Table 5-2: Service Level Objectives

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 and formalised through Service Level Management. They must be reviewed periodically, at least once per year, to ensure that they are still current and aligned to business needs. It is therefore recommended to develop a formal review schedule which should be incorporated into the TES IT Service continuity plan and the appropriate SLA.

A common approach should be defined and applied per application in scope. This will stimulate uniformity and enable a consistent and pragmatic pan-European application of these service level objectives. It must be noted that the type and implementation of technology might prevent a uniform approach, this remains to be investigated at a later stage.

5.3.5 Gap Assessment Requirements

As mentioned before there is a need to conduct a more thorough and goal oriented assessment in order to obtain an objective view of the status within Member States. Only then will the ITSM contractor be in the position to identify areas for improvement that contribute to achieving the objectives of the IT Service continuity plan.

The assessment should target specific areas of interest in order to meet the objectives of the recommended initiatives. It should also be a useful management tool in measuring progress over time and in establishing improvement targets and objectives that can be managed through the continuous service improvement program.

The table below presents the initial proposed target areas that need to be assessed as part of this plan.

Ref	Target area	Description
AR1	Recovery objectives (the agreed objectives will be used to compare against)	Business and system recovery objectives should be analysed and compared, if and where appropriate, to determine if any gaps exist in the capabilities of the Member States. Possible gaps between the agreed RPO's and current RPO's within the Member States, if and where appropriate, should be determined in order to understand current capabilities.
AR2	Recovery strategy (the agreed strategies will be used to compare against)	The final agreed recovery strategies should be compared to existing strategies within Member States and the gap between the established requirements and current capabilities determined.

Table 5-3: Proposed gap assessment target areas

The above assessment covers only a small set of aspects of IT Service continuity management capabilities. In order to gain a more comprehensive view of the status of current capabilities within the Member States, a more thorough assessment in the form of a gap analysis must be conducted. This gap analysis can be managed through the CSIP and subsequently incremental improvements realised over time.

However, one of the main prerequisites of such a gap analysis is the establishment of the requirements and scope covering the various continuity management aspects and the use of a comprehensive questionnaire to facilitate information gathering.

5.4 Action Plan

The following is an outline of the envisioned next steps underpinning the vision in the realisation of the next iteration of the TES IT Service continuity plan and those aspects mentioned in this document.

5.4.1 ITSCM Working Group

An ITSCM working group involving Member State representatives and CCN/TC has to be implemented as a pre-requisite to the TES IT Service continuity plan realisation. In particular, the working group will help in driving decisions and assisting in the development of appropriate standards and approaches where required.

CCN/TC plays a key role in this working group due to the interfacing between the CCN BCP plan and the Member State plans. Defining the perimeters of responsibilities between the Member States, CCN/TC, ITSM contractor and DG TAXUD IT is a key issue to be addressed in order to ensure that plans are fully aligned and the responsibilities of the involved parties are documented accordingly. The scope, which is

broad, needs to be tightened and the challenge will be the integration and interoperability between the Commission effort and the NAs efforts.

The composition of the working group should be established through collaboration with the Member States, CCN/TC, ITSM contractor and DG TAXUD. Once the final composition of the working group is defined, DG TAXUD will, of course, have a leading role in this working group.

5.4.2 Workshops

Several workshops and meetings with stakeholders and Member State representatives should be conducted with each aligned to specific goals and objectives. The scope, objectives and amount of workshops depends on the final agreed initiatives as a result of this plan and remain to be determined at a later stage. At a minimum the following workshops are required in order to produce the deliverables set out in this chapter:

1. Business impact assessment definition and method workshop;
2. Risk analysis definition and method workshop;
3. Business impact assessment and RTO workshop;
4. Application classification and availability requirements workshop;
5. Recovery strategies workshop;
6. Service level objectives workshop.

The participants of the workshops remain to be identified. At a minimum the business sector leaders, business perspective managers and the ITSM contractor continuity manager or designated backup will have to attend the workshops. In addition, the ITSM Availability, Capacity and Service Level manager will, as required, attend the workshops as well.

5.4.3 Gap assessment

The sample questions listed in Annex B will, upon approval of DG TAXUD, be formalised and submitted to Member State contacts. It must be noted that prior to sending the questionnaire, the requirements for the different target areas mentioned in Section 5.4 should have already been established and formalised. The assessment process consists of the following steps:

Step 1 – Develop assessment questionnaire form

Develop questionnaire form with as much multiple choice questions as possible and submit to DG TAXUD for approval. Include agreed continuity requirements and definitions to ensure consistent use and application of terminology.

Step 2 – Information gathering

Identify owners and locations, submit questionnaire and start collecting information using the questionnaire. Issue e-mail from DG TAXUD and provide the ITSM contractor contact details.

Step 3 – Information processing

During this step the information is processed. Unaligned information or discrepancies are rationalised and made consistent, and remaining gaps identified. The goal of this step is to process the information from multiple disparate sources into an "apples to apples" comparison. Once the information is rationalised, the analysis will start.

Step 4 – Analyse Information

Here the raw information becomes useful information as it is analysed to identify the actual readiness status of Member States against the requirements. The variance between the requirements and current capabilities (baseline) is determined, documented and approved.

Step 5 – Recommendations

Here the results and recommendations are presented to the various stakeholders and the improvement efforts proposed in a form and manner that reflects the objectives of the TES continuity plan. Action plans for improvements are developed and agreed.

5.5 Planning

This section contains an overview of the stages and activities involved in the realisation of the proposed activities. The proposed stages are indicative and remain to be worked out into a proper project plan once agreed by DG TAXUD and the Member State representatives. The assumption is made that the activities as a result of the recommended initiatives should be completed within six months after acceptance of this document by DG TAXUD in order to be completed by the next evolutive version.

The planning consists of three main stages. The table below lists the stages, high level activities, and target completion dates involved in the realisation of the initiatives and the deliverables part of the recommendations. For the purpose of planning a default starting time value (T0[8]) is used.

[8] T0 is defined as the time at which this plan is formally accepted by TAXUD.

Stage 1	Description of activities	Target
Business requirements	Business impact definition and method workshop Risk analysis definition and method workshop Business impact analysis workshop Availability and classification workshop RTO workshop Service level objectives workshop RPO analysis and confirmation	T0+4 months

Stage 2	Description of activities	Target
Assessment	Develop gap assessment questionnaire Develop risk analysis questionnaire Information gathering Information processing Information analysis Gap recommendations Produce risk analysis report and recommended risk response measures	T0+6 months

Stage 3	Description of activities	Target
Formalise evolutive version of the IT Service Continuity Plan	Update plan based on new developments Add new recommendations and guidelines	T0+10 months

This document proposes already a start for IT Service Continuity, but it will not be possible to go to implementation phase without commitment from all parties to provide inputs (which is illustrated in section 5.2) to achieve the goal of this document

A.1 STATUS OVERVIEW CUSTOMS

Country	Status	Date
Andorra	See Extract mission report for details.	October 2007
Austria	No information received since date mentioned, follow up required.	November 2008
Belgium	No information received since date mentioned, follow up required.	November 2008
Bulgaria	See extract mission report for details.	October 2009
Cyprus	See extract mission report for details.	November 2007
Czech Republic	See extract mission report for details.	January 2008
Denmark	See extract mission report for details.	November 2007
Estonia	See extract mission report for details.	March 2008
Finland	See extract mission report for details.	March 2008
France	No information received since date mentioned, follow up required.	November 2008
Germany	No information received since date mentioned, follow up required.	November 2008
Great Britain	See extract mission report for details.	January 2008
Greece	See extract mission report for details.	November 2007
Hungary	See extract mission report for details.	December 2007
Ireland	No BCP/DRP exists.	November 2008
Italy	See extract mission report for details.	October 2007
Latvia	See extract mission report for details.	November 2007
Lithuania	See extract mission report for details.	March 2008
Luxembourg	No information received since date mentioned, follow up required.	November 2008
Malta	See extract mission report for details.	October 2007
Netherlands	No information received since date mentioned, follow up required.	November 2008
Norway	See extract mission report for details.	May 2008
Poland	See extract mission report for details.	March 2008
Portugal	No information received since date mentioned, follow up required.	November 2008
Romania	No information received since date	November 2008

	mentioned, follow up required.	
San Marino	See extract mission report for details.	October 2007
Slovakia	See extract mission report for details.	January 2008
Slovenia	No information received since date mentioned, follow up required.	November 2008
Spain	No information received since date mentioned, follow up required.	November 2008
Sweden	See extract mission report for details.	February 2008

Country:	Bulgaria
Source:	Extract from **Liaison mission report to NA-BG (ITS-IMRP-004-NA-BG)** of visit on 14/09/2009
Extract:	The new BG Government decided to significantly reduce the number of BCA staff (at the time of this mission, a reduction of 400 – 500 members of staff was discussed) and at the same time to dedicate additional tasks (like road tax control) to BCA. Furthermore and due to the credit crunch, a temporary budgetary cut of up to 40% applied to BCA projects on IT development and maintenance. Seen aforementioned significant reduction of BCA staff and the required further streamlining of BCA business processes, on-going projects on major Customs Trans-European Systems and the expected considerable impact of the Modernised Customs Code on IT environments of EC National Customs Administrations, Bulgaria should ensure adequate human and financial resources for BCA IT administrative capacity and IT projects. Furthermore and seen the complexity and increasing importance of BCA IT systems for the common, national and external domain, BCA should proceed with their project on implementing a DRC at Plovdiv Regional Customs House in line with the Terms of Collaboration and Service Level Agreement between the European Commission and the EC National Ministries of Finance.

Country:	Czech Republic
Source:	Extract from CPT mission report **TAXUD-A3/ECUST/MD D(2008) 5244 AN**, of visit on 24/1/2008
Extract:	Czech ACM documentation is comprehensive and complete, except for disaster recovery planning. However, at the time of the mission also for the latter ACM part a draft version existed. The completion of this ACM task is however largely depending on an instable positioning of the Czech Government on whether installing and operating a Disaster Recovery Centre (DRC) or not. With a basic go/no-go decision for a DRC pending on Czech Government level for years, CCA has defined a solution, which outlines disaster recovery for software components (application and database) but

	which is relying on leasing / procuring new hardware components in case of a disaster scenario. This approach however leaves risk as to the prioritisation of recovery of system operations (days/weeks).

Country:	Cyprus
Source:	Extract from CPT mission report **TAXUD-A3/ECUST/MD D(2007) 5033 AN**, of visit on 16/11/2007
Extract:	ACM requirements are complete and satisfactorily documented for national Cypriot NCTS (and ECS) operations.

Country:	Denmark
Source:	Extract from CPT mission report **TAXUD A3/ECUST/MD D(2007) 4884 AN**, of visit on 8/11/2007
Extract:	National Danish ACM (NCTS & ECS) documentation is complete. The Disaster Recovery Plan and Crisis Escalation Management have been well defined including roles. However**,** the envisaged SLA with the selected maintenance & monitoring framework contractor should be signed without any further delays, so as to fully stabilise ACM for NTA-DK and NECA-DK. In this exercise, SKAT should finally decide whether national CCN administration shall be outsourced or not.

Country:	Estonia
Source:	Extract from CPT mission report **TAXUD A3/ECUST/MD(2008) 5660**, of visit on 17/3/2008
Extract:	Estonian ACM documentation for NCTS and ECS is comprehensive and complete; it clearly defines and describes in detail internal and external roles, workflows and information channels for crisis and escalation management. Since the most recent CPT liaison mission to Estonia in March 2006 the witnessed significantly increased availability of NTA-EE (and as from start of international operations of NECA-EE) can be regarded as quality indicator for the effectiveness of those ACM workflows and crisis & escalation management. As regards Disaster Recovery Planning, a physical separation of NTA-EE and NECA-EE operational and testing / backup servers, into two independent premises has been envisaged but was at the time of the mission not yet reflected into the (mid-term) IT Strategy of the Estonian Tax and Customs Board (EMTA).

Country:	Finland
Source:	Extract from CPT mission report **TAXUD A3/ECUST/MD(2008) 5658**, of visit on 12/3/2008 and 13/3/2008
Extract:	Finnish ACM documentation for NCTS and ECS is comprehensive and complete; it clearly defines and describes in detail internal and external roles, workflows and information channels for crisis & escalation management.

Country:	Great Britain
Source:	Extract from CPT mission report **TAXUD-A3/ECUST/MD D(2008) 5243 AN**, of visit on 14/1/2008
Extract:	H.M. Revenue & Customs (HMRC) orientates at ITIL standards, and therefore ACM requirements are well met in the United Kingdom. However, as regards disaster recovery planning for NTA-UK, HMRC senior management underlined that this would be pointless, as for certain key services that the NTA-UK national domain depends upon (in particular EDCS, web and XML channels) no disaster recovery is foreseen by the British Government. However, NPT has secured quality Service Level Agreements with HMRC Pre-Production Environment (PPE) Services (competent for ECDS, web and xml channels) and outsourced Services for HMRC infrastructure.

Country:	Greece
Source:	Extract from CPT mission report **TAXUD A3/ECUST/MD D(2007) 70091 AN**, of visit on 20/11/2007
Extract:	As regards national Availability & Continuity Management, CPT appreciates the planning of NPT to complete and adopt documentation on Crisis & Escalation Management for NTA-GR (and NECAGR) by end December 2007. The same planning should preferably also be met for completing and adoption of the Disaster Recovery Plan (DRP) for the Greek Ministry of Economics and Finance, which however is not in the portfolio of NPT. Therefore, GSIS senior management should invite the competent GSIS services to implement DRP without any further delays. The development of a (sophisticated) monitoring system under the project on the new Centralised Greek Customs Information System (Centralised ICIS) is indispensable and should be implemented as early as possible.

Country:	Hungary
Source:	Extract from CPT mission report **TAXUD A3/ECUST/MD(2008) 5024 AN**, of visit on 17/12/2007
Extract:	The Hungarian Customs and Finance Guard (VIG) is planning to implement in S1/2008 a single unavailability system for all its IT applications; the national Hungarian documentation on Crisis & Escalation Management (including roles and workflows) will be completed in line once that the latter unavailability system will have been implemented. VIG is furthermore planning to have in place a new IT Centre by mid 2008, which shall be installed in the premises of the Budapest Regional Customs House and which will be based on a new IT platform for NCTS phase-4 and ECS phase-2. The present operational VIG IT Centre will be operating the future fallback server farms. The Disaster Recovery Plan will be adapted to these new structures. At the time of the mission information stability and integrity were unsured through automatic replication and backup-up mechanisms.

Country:	Italy
Source:	Extract from CPT mission report **TAXUD A3/ECUST/MDD(2007)4751 AN**, of visit on 4/10/2007 and 5/10/2007
Extract:	ACM requirements are implemented best practice in Italy. Only as regards continuity of the national NCTS and ECS projects, certain risks remain to meet the defined operational deadlines for abovementioned NCTS and ECS evolutions (1st January and 1st July 2009), where a) in the case of NCTS/TIR procedural constraints for partial un-loading/up-loading of goods have been remaining on Italian side since the 5th NCTS Evaluation Workshop (June 2006) and where b) in the case of NCTS security and ECS phase-2 Italy requires significantly stabilised functional specifications for the EORI system, due to its anticipated effects on NCTS security and ECS phase-2. TAXUD/C

	is requested to solve these pending issues with Italy.

Country:	Latvia
Source:	Extract from CPT mission report **TAXUD-A3/ECUST/MD D(2007)5062 AN,** of visit on 29/11/2007
Extract:	National Latvian ACM documentation on Crisis & Escalation Management for NCTS and ECS (CEM) and on a Disaster Recovery Plan (DRP) is complete and has been well defined, including roles. However, a continuous up-date of linking members of staff of the SRS IT Department in particular with CEM roles remains essential, as again a considerable turn-over of (experienced) SRS IT administrators was registered since the most recent CPT liaison mission. Latvian SRS reached a new agreement with the NTA/NECA-LV developer to guarantee support also outside core working hours as from the implementation of CDTA/CDXA v. 6xx in Latvia, which should ensure in the future scheduling unavailability outside ACM business hours. CPT regretted to learn that the recruitment procedure for 6 additional members of staff, planned for July 2007, for 24h/24h monitoring with physical presence of all SRS IT applications was only marginally successful and that posts, for which no new members of staff could be recruited, were cut by the Latvian Government prior to this liaison mission. SRS should aim at requesting a new recruitment exercise for missing monitoring administrators

Country:	Lithuania
Source:	Extract from CPT mission report **TAXUD A3/ECUST/MD(2008) 5992 AN**, of visit on 31/3/2008
Extract:	Lithuanian ACM documentation is comprehensive and complete including defined roles and contact points. National statistics for unscheduled unavailability of NTA-LT and NECA-LT in the year 2007 demonstrated that ACM has been soundly implemented in Lithuania. As regards Disaster Recovery Planning, LT Customs have installed two redundant and physically separated data centres. The NTA and NECA-LT operational environments have been clustered in these data centres. At the time of the mission NTA and NECA test environments were separated in the two data centres but not yet clustered. Considerable risks to the sustainability of NTA and NECA-LT support and quality operations have been identified by the severe knowledge attrition in the Lithuanian NCTS and ECS National Project Teams in the year prior to this mission, which could jeopardise future Lithuanian quality NCTS and ECS operations in the external, national and common domain and therefore could also have a negative impact on other EU Member States and other

	contracting parties of the Common Transit Convention. While LT Customs have taken first mitigation steps taken to address this risk, the Lithuanian Customs Department should take further necessary steps to ensure that in particular the IT knowledge and skills built up by the Lithuanian National Project Teams in setting up NCTS and ECS are secured for the foreseeable future. Furthermore, the availability of appropriate resources has been identified as severe risk for the overall continuity of the Lithuanian Customs project that mainly orientates at the current revision 8 of the Multi-Annual Strategic Planning, and which is furthermore directly linked to the envisaged new Lithuanian Customs Declaration Processing System (CDPS). To deliver all complex system adaptations and developments ahead of the Lithuanian Customs Administration, the Lithuania Customs Department should therefore take all necessary steps to ensure the availability of appropriate resources in the future.

Country:	Malta
Source:	Extract from CPT mission report **TAXUD-A3/ECUST/MD D(2007)4759 AN**, of visit on 12/10/2007
Extract:	NCTS operations represent in all sectors good and stable practice. In certain areas, Maltese NCTS operations present best practice, in particular on CCN and NTA availability as well as on the technical error rate. In the reporting period, NPTs significantly invested in up-grading the power networking and UPS systems to tackle the frequent power failures in Malta. Furthermore, Malta had identified last outstanding single points of failure as regards mirroring disks, which are planned to be overcome in the near future. ACM requirements are complete, well documented and well met in Malta.
Source:	Extract from CPT mission report **TAXUD-A3/ECUST/MD D(2008) 6575 AN**, of visit on 2/6/2008
Extract:	The single point of failure in the context of ACM for NCTS-MT as identified in the most recent CPT liaison mission has been overcome. ACM documentation and crisis & escalation workflows for ECS-MT will be completed after the expansion of the Terms of Collaboration – Specifications for implementing availability and continuity in NCTS v. 1.07 of 7/07/2006 (ToC ACM) – to all other Customs Trans-European Systems.

Country:	Norway
Source:	Extract from CPT mission report **TAXUD A3/ECUST/MD(2008) 5625 AN**, of visit on 19/5/2008 and 20/5/2008
Extract:	Norwegian ACM documentation is comprehensive and complete including clearly defined roles and NCA internal and external contact points. Crisis & escalation planning covers all IT systems of the Norwegian Customs

	Administration (NCA). As regards Disaster Recovery Planning, a full NTA-NO crisis back-up system has been installed in the premises of the selected NCA contractor for NCA IT infrastructure and is connected by fibre channel to the production environment of NTA-NO. Monitoring of all critical services and components of all NCA IT systems (including NTA-NO) are secured 24h/24h.

Country:	Poland
Source:	Extract from CPT mission report **TAXUD-A3/ECUST/MD D(2008) 5979 AN and TAXUD-A3/ECUST/MD D(2008) 5980 AN**, of visit on 27/3/2008
Extract:	**ECS and ICS NPT:** Internal procedures for ACM for NECA-PL have been set up including defined roles and contact points. Comprehensive technical ACM documentation for NECA-PL in form of an Operational Level Agreement is still under development. NPT was at the time of this mission planning to install a back-up centre for NECA-PL in Lodz, which had been already orally confirmed by PL MoF IT Services. During this mission, however, the representative of the PL MoF IT Services informed CPT about alternative plans to install such a backup centre in expanded server vaults in the premises of the PL MoF. Poland has been requested to reconfirm its final decision in the near future, so as to better meet Disaster Recovery Planning for NECA-PL without any further delays. Particular risks for continuity of NECA-PL development & maintenance have been identified by a delayed tendering procedure for the envisaged new development & maintenance contract for ECS phase-2 and ICS phase-1 in Poland. A start of this envisaged contract at the latest by 1st September 2008 will be critical for ECS phase-1 maintenance in Poland as well as essential in light of the short remaining implementation period for ECS phase-2 and ICS phase-1 in Poland. Further technical risks for NECA-PL application servers have been identified with the pending decision whether the maintenance contract for the selected JBoss architecture will be prolonged at the latest by end November 2008 as proposed by (at least) another year. The competent IT Services in the PL MoF have been requested to address these two issues with maximum momentum. Further considerable risks to the sustainability of NECA-PL support and quality operations have been identified with the significant attrition of knowledge related to the NECA IT administration in the year prior to this liaison mission. This had particular impact on 24h/24h in-house NECA-PL monitoring and support as well as on technical NHD level-2. **NCTS NPT:** Polish ACM documentation is comprehensive and complete including defined roles and contact points.

	However, with an installation of a Disaster Recovery Centre for all Polish Customs and Tax systems pending on ministerial level for years, currently prevention of NTA-PL data sustainability in disaster situations is mainly relying on full daily back-up cycles, several redundant NTA-PL back-up services and on disaster recovery for software components (application and database). As regards hardware, procurement of new components in case of a disaster scenario is foreseen; however, this approach leaves risks as to the prioritisation of recovery of system operations (days / weeks).

Country:	Slovakia
Source:	Extract from CPT mission report **TAXUD-A3/ECUST/MD D(2008) 5246 AN**, of visit on 22/1/2008
Extract:	Slovak ACM documentation is comprehensive and complete. For NECA-SK generic documentation applies as NECA-SK is fully integrated into the Slovak Customs Declaration Processing System (ISST-DS). Separate ACM documentation was set up for NTA-SK, as this system is (not yet) integrated into ISST-DS.

Country:	Sweden
Source:	Extract from CPT mission report **TAXUD A3/ECUST/MD(2008) 5380 AN**, of visit on 6/2/2008
Extract:	Swedish ACM documentation is comprehensive and complete. NECA-SE is fully integrated into the Swedish Customs Declaration Processing System (CTS), which is not the case for NTA-SE. Therefore, for certain areas ACM documentation for NTA-SE varies from the related generic CTS documentation. As regards disaster recovery planning, Swedish Customs IT Services (Tulldata) installed in autumn 2006 a second high availability data centre 12km away from its own premises.

A.2 ASSESSMENT QUESTIONNAIRE

Sample Assessment Questions

Area	Questions
Recovery Objectives	Are you familiar with the terms business recovery time objectives and system recovery time objectives?
	Are existing or future recovery plans capable of supporting the established business recovery objectives?
	Do current recovery plans contain system recovery time objectives and priorities? If yes, will these need to be adjusted based on the new business recovery time objectives? Please elaborate.
	Are current or future (project) plans capable of meeting the established recovery point objectives? Please list the currently implemented RPO's per application.
Area	**Questions**
Recovery Strategy	Are different recovery strategies currently in place for the applications part of the business thread or being planned as part of a project?
	Please provide a list with all current implemented strategies per application listed in the attached file.
	Do you foresee any problems with aligning local strategies, if applicable, to the agreed pan-European strategies? Please elaborate.

A.3 BUSINESS IMPACT MATRIX (SAMPLE)

e.g. MVS		Service Outage Time bands				
Impact Type	**Impact level**	**2 hours**	**24 hours**	**48 hours**	**96 hours**	**168 hours**
Operational	5 More than 1,000 employee hours					
	4 Between 500 and 1,000 employee hours					
	3 Between 100 and 500 employee hours					
	2 Between 10 and 100 employee hours					
	1 Less than 10 employee hours					
Financial	5 More than €10 million					
	4 Between €1 million and €10 million					
	3 Between €100 thousand and €1 million					
	2 Between €10 thousand and €100 thousand					
	1 Less than €10 thousand					
Political/Image	5 Negative exposure by major media and/or possible major government sanctions					
	4 Negative exposure by minor media and/or possible minor government sanctions					
	3 Negative exposure by word of mouth and/or breach of regulations					
	2 Negative exposure by word of mouth and/or breach of internal policies					
	1 No publicity or violation of rules					
Impaired Strategy	5 Strategic initiative aborted					
	4 Strategic initiative delayed by 2 months or more					
	3 Strategic initiative delayed by less than 2 months, but by more than 2 weeks					

e.g. MVS		Service Outage Time bands				
Impact Type	**Impact level**	**2 hours**	**24 hours**	**48 hours**	**96 hours**	**168 hours**
	2 Strategic initiative delayed by 2 weeks or less					
	1 Strategic initiatives not impacted					
Total impact level						

A.4 STATUS OVERVIEW TAXATION

Country	Status	Date
Austria	No BCP project, no risk assessments done. Tested procedures in place for back-up and fail-over of systems.	September 2008
Belgium	Nothing in place for BCP/DRP as far as TAXUD applications is concerned (VIES Belgium). Belgian Customs infrastructure is redundant, in separate datacenters (12 km), except for the gateways (production and back-up) which currently are in same room as per Commission instructions	September 2008
Bulgaria	No separate plan, but procedures are in place. Have not been communicated, but have been tested.	September 2008
Cyprus	Waiting on information, follow up required.	November 2008
Czech Republic	No specific DRP/BCP for VIES, but procedures in place for SW/HW/Network failures. The Infrastructure is redundant.	September 2008
Denmark	Waiting on information, follow up required.	November 2008
Estonia	Estonian Tax and Customs Boards System Maintenance Department has a documented Disaster Recovery Plan. Plans have been communicated to all interested parts of the organisation and are maintained by the System Maintenance Department. Scope of the DRP plans are servers and data and tests are performed according to the plans.	September 2008
Finland	BCP project on-going. No DRP exists at this stage. Partial recovery plans per system exist. Tests are being conducted ad-hoc. Infrastructure is redundant and spread across two computer rooms.	November 2008
France	Nothing exists, but study will be conducted in 12/2008, to be finished mid 2009, after which implementation project (over 3 years) will start).	September 2008
Germany	BCP/DRP exists; it has been communicated and is maintained. The scope however does not include VIES. Procedures are available and the Infrastructure is redundant.	September 2008

Country	Status	Date
Great Britain	DRP is in place, tests are executed. VIES, CCN/CSI is covered. Production is backed-up with a twin system, in different locations (except of the gateways). Migration project ongoing to a new datacenter.	September 2008
Greece	Requested a questionnaire to work with the technicians.	
Hungary	Waiting on information, follow up required.	November 2008
Ireland	Formal BCP plans are currently being put in place for Revenue key priority systems. The BC system will be in accordance with British Standard BS25999-2:2007 Business Continuity Management & ISO27001 Information Security Management. The current scope of the system will be Revenue's Internet facing systems and the core Integration Taxation System. Initially it will not include the onward transmission of data from Ireland to the EU. The connectivity systems for CCN belong to the EU and are situated in a single site. There is no connectivity provided from our alternative site. It will be communicated within Revenue. As EU systems are not initially within scope it will not be communicated to EU. It will be maintained as required by BS25999-2:2007 & ISO27001 Information Security Management. Desktop exercises and isolated system recoveries for some of the applications within scope have been carried out. The current scope of the system will be Revenue's Internet facing systems and the core Integration Taxation System. It does not include onward transmission to the EU.	September 2008
Italy	Waiting on information, follow up required.	November 2008
Latvia	No BCP exists, however there are 18 DRP's covering various applications with detailed recovery procedures. There are no stand-by arrangements, backups are made daily. The plans are communicated within IT. Procedures have been tested and are maintained through change management.	September 2008
Lithuania	Waiting on information, follow up required.	November 2008
Luxembourg	Waiting on information, follow up required.	November 2008

Country	Status	Date
Malta	Waiting on information, follow up required.	November 2008
Netherlands	Waiting on information, follow up required.	November 2008
Norway	Waiting on information, follow up required.	November 2008
Poland	Waiting on information, follow up required.	
Portugal	Business Continuity Plan and/or Disaster Recovery Plans doesn't exist yet but there are intentions in future to have these plans.	November 2008
Romania	Nothing in place, but project will be started to have DRP/BCP by late 2009.	September 2008
San Marino	Waiting on information, follow up required.	
Slovakia	We had prepared working versions of BCP/DRP documents but they weren't published. Taking into account the changes in our system architecture two years ago and the establishment of new working positions for security manager and IT security manager in our administration, these documents are already not up to date. So, nowadays we are in a position of reviewing and creating documents related to security. On the basics of these documents a new Business Continuity Plan and Disaster Recovery Plans will be prepared.	September 2008
Slovenia	No BCP in place and no planning in place.	September 2008
Spain	Waiting on information, follow up required.	November 2008
Sweden	Everything is redundant, there should be no issues, and recovery is planned within a few hours.	September 2008