OWNER:	ISSUE DATE:	VERSION:
DG TAXUD	30/04/2010	1.05

TAXATION AND CUSTOMS UNION DG
ITSM

SUBJECT:

Security Plan for the IT services related to trans-European systems managed by the Commission and the Member States

REF: ITS-IPLN-SEC-SC06-004

FRAMEWORK CONTRACT # TAXUD/2007/CC/088

SPECIFIC CONTRACT 06

[Blank for duplex printing]

DOCUMENT HISTORY

Edi.	Rev.	Date	Description	Action (*)	Pages
0	01	27/11/2008	First Draft – delivered for internal QC	I	All
1	00	28/11/2008	Submitted for Review	I, R	All
1	01	15/12/2008	Submitted for Approval	I, R	All
1	02	19/12/2008	SfA; modify as discussed with LISO on 16 Dec 08	R	20, 21
1	03	02/04/2010	Modify as discussed with LISO on 22 Mar 2010; internal QC	I, R	As required
1	04	09/04/2010	SfR	I, R	As required
1	05	30/04/2010	SfA	I, R	As required

(*) Action: I = Insert R = Replace

Table of Contents

Table of Tables

Tables of Figures

1. Introduction

1.1 Objective of Document

This document defines how the ITSM Contractor is managing security related to Trans-European IT services provided to DG TAXUD in the framework of the ITSM project. This is the Deliverable DLV.8.5.5 "Security Plan for the IT services related to trans-European systems managed by the Commission and the Member States" identified in Specific Contract 06 of Framework Contract TAXUD/2007/CC/C088, Work Package W.P.8.5.

This document describes the processes carried out by ITSM Security Management in the scope of the Trans-European Services.

1.2 Scope of Document

The scope includes the IT and network equipment, as well as the security procedures and standards that make part of the systems described in the following paragraphs of applicable document AD3:

- § 3.4.1 (Distributed TES model);
- § 3.4.2 (Centralised TES).

1.3 Target Audience

The intended audience of this document is:

- ITSM Contractor;
- QAC;
- DG TAXUD;

1.4 Business Context

DG TAXUD is responsible for the provision of a wide portfolio of trans-European and Commission central IT services to the National Administrations (NA), the public and the Commission internal staff.

The ITSM project is concerned with:

- Providing IT services management for all existing and future trans-European and Commission central systems of DG TAXUD;
- Consolidating the diversity of all the current IT service management processes into a single set of processes.

1.5 Abbreviations and Acronyms

Acronym	Description
DG	Directorate General
DG TAXUD	Directorate General TAXUD: Taxation and Customs Union
EC	European Community
ISO	International Standardisation Organisation
ISO/IEC	International Organisation for Standardisation / International Electrotechnical Commission
ISSP	Information System Security Policy
ITSCM	IT Services Continuity Management
ITSM	Information Technology Service Management
LISO	Local Informatics Security Officer
LSA	Local System Administrator
NA	National Administration
NISO	National Information Security Officer
NPM	National Project Manager
RFC	Request for Comment
TEMPO	TAXUD Electronic Management of Projects On-line
ToC	Terms of Collaboration

Table 1: Abbreviations and acronyms

1.6 Glossary

The terms used in this document are compliant with the ITSM Glossary [RD2]. This Glossary has been developed to provide a common language throughout the ITSM project and to avoid confusion over local or national differences in terminology.

1.7 Reference Documents

Ref.	Title	Originator	Version	Date
[RD1]	Information technology – Security techniques – Code of practice for information security management. ISO/IEC 27002:2007	ISO/IEC	1.00	Jun 2005
[RD2]	ITSM – Glossary of terms	ITSM Contractor	1.11	Feb 2010

Ref.	Title	Originator	Version	Date
[RD3]	Information technology – Security techniques - Information security management systems – Requirements ISO/IEC 27001:2005	ISO/IEC	1.00	Oct 2005

Table 2: Reference documents

1.8 Applicable Documents

An applicable document is a document of which the content is binding for the contractor in the context of this document.

Ref.	Title	Originator	Version	Date
[AD1]	TEMPO – User Account Management Procedure	DG TAXUD /A3	1.40	17/01/2008
[AD2]	Framework Quality Plan, deliverable DLV.0.1.2 of the ITSM project	ITSM	1.04	22/03/2010
[AD3]	TEMPO – Trans-European Systems Reference Manual	DG TAXUD /A3	1.21	Mar 2009
[AD4]	Technical Annex to the Model Framework Contract of ITT TAXUD/2006/AO-007	DG TAXUD /A3	1.00	Jul 2006

Table 3: Applicable documents

2. Security Management Processes

The top security management processes for Trans-European Services are represented in the diagram below. The relative positions of the processes in Figure 1 do not imply that the processes must be carried out in the sequence shown:

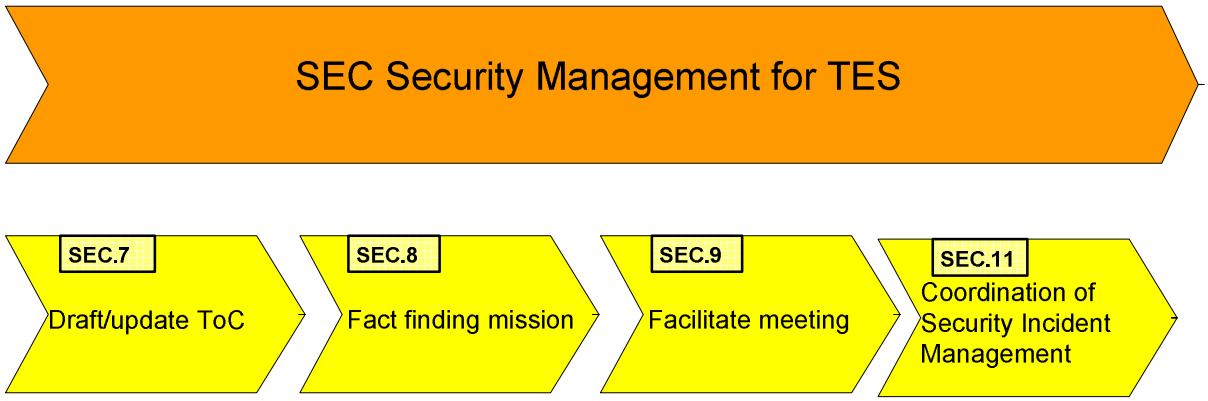

Figure 1: Overall Security Management Processes

The processes shown in the figure above are further described in the next sections.

3. Draft/ Update ToC

The “draft/ update ToC” service is provided by ITSM Security Management to DG TAXUD.

3.1 Scope

The scope of this service includes the security-related part of ToC (Terms of Collaboration). According to applicable document AD4, §2.7, “*The Terms of Collaboration define the mutual obligations of the NAs and the Commission around the Common Domain*”. A ToC document concerns identified user communities within identified business threads in identified Member States.

3.2 Process

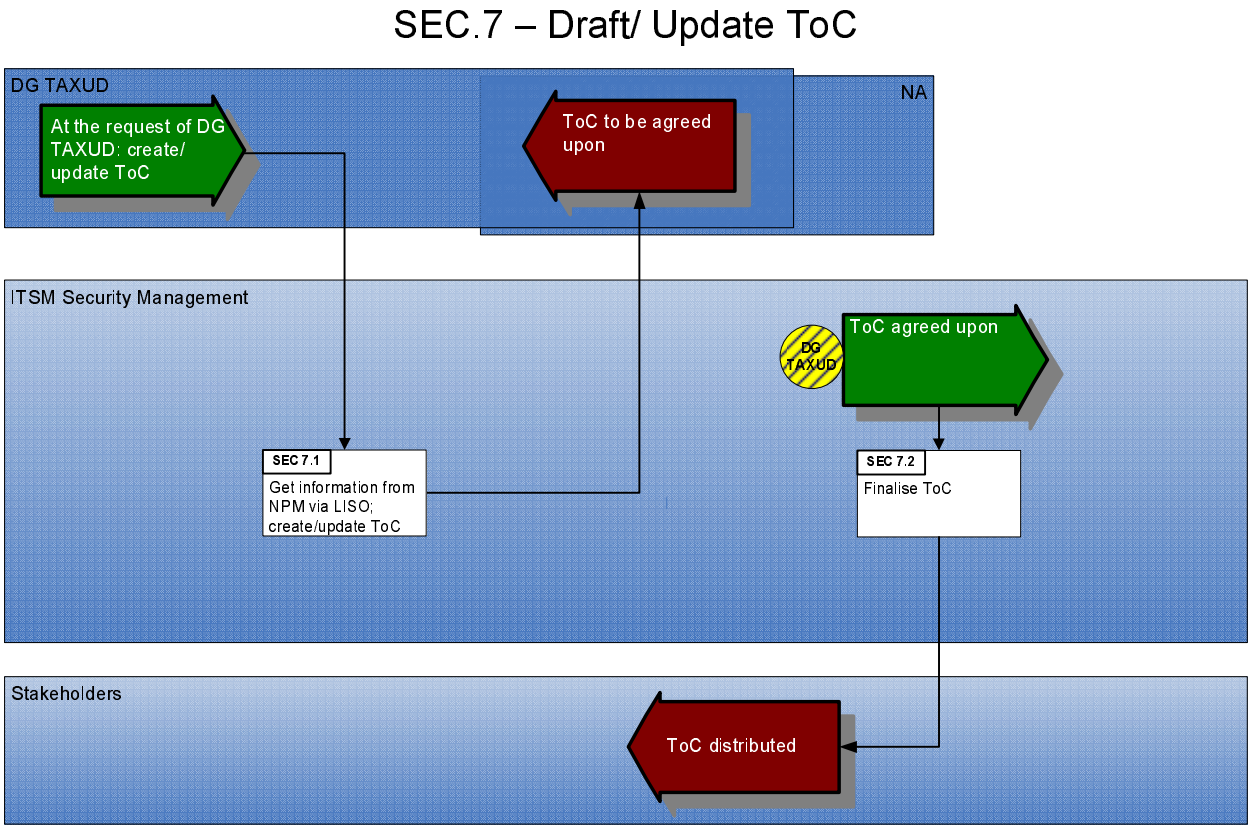

Figure 2: Draft/update ToC Process

The process starts on a request from DG TAXUD to create/ update ToC documents. DG TAXUD identifies the concerned user communities, the concerned business threads, and the concerned Member States. The process is executed by ITSM Security Management, who provides the following services:

- Update security-related part of ToC (in case it already exists), or create security-related part of ToC (in case it is new). See proposed contents in §3.4 below;
- Submit created/ updated ToC to DG TAXUD LISO for review/ for approval;
- Distribute approved ToC to stakeholders, i.e. to:
  - DG TAXUD LISO
  - NAs

3.3 Roles and Responsibilities

The involved parties are:

- DG TAXUD LISO;
- NAs, through the concerned NPMs, who may delegate someone else to represent them;
- ITSM Security Management.

The roles and responsibilities in the frame of the Draft/ Update ToC service are as follows:

Role	Responsibilities
DG TAXUD LISO	• Provides common standards on the security of TES, and enforces them through ToC; • Agrees with the involved NAs about the terms and conditions under which they collaborate with DG TAXUD in the field of security; • Reviews/ approves the security-related part of ToC.
NPM	The NPM in each involved NA shall: • Nominate a delegate if needed. The delegate shall have the same authority as the NPM regarding the topics that are addressed in the security-related part of the ToC; • Provide DG TAXUD LISO with the capacity/ continuity/ availability/ security plans that are currently in effect in their environment; • Cooperate with DG TAXUD LISO and with ITSM Security Management to reach an agreement on ToC, which explicitly document terms of collaboration between his user community and DG TAXUD on the field of security.
ITSM Security	• Coordinates the development and the delivery of the security-

Management	related parts of ToC documents; • Provides technical expertise during the drafting of the security-related parts of ToC documents.

Table 4: Roles and Responsibilities for “Draft/ Update ToC” process

3.4 Deliverable

The contents of the security-related part of ToC need to be agreed upon between DG TAXUD LISO, the involved NAs and ITSM Security Management on a case-by-case basis. Generally the contents are:

- Roles and responsibilities of DG TAXUD and the NAs in the field of security;
- Statement of compliance of the ToC with the SLA from the NAs to DG TAXUD and —conversely— the SLA from DG TAXUD to the NAs;
- Reference to capacity/ continuity/ availability/ security plans applicable to the Common Domain and to the Local Domain;
- Terms and conditions under which DG TAXUD and the NAs will collaborate to:
    - Coordinate their efforts on the risk management of TES;
    - Harmonise security controls across Trans-European Systems;
    - Raise awareness about information security within NA personnel;
    - Promote best practices in the field of information security.

4. Fact Finding Mission

4.1 Scope

The scope of this service includes fact-finding missions as required by applicable document AD4, §1.2-WP8.5: ITSM shall "*perform fact finding missions in the NAs and 3rd parties to note their security controls in place*". A fact-finding mission concerns identified user communities within identified business threads in identified Member States.

An example of a fact-finding mission is: ad-hoc activities (e.g., review of security implementations), which are requested by DG TAXUD LISO, and which are related to the security of Trans-European Systems.

4.2 Process

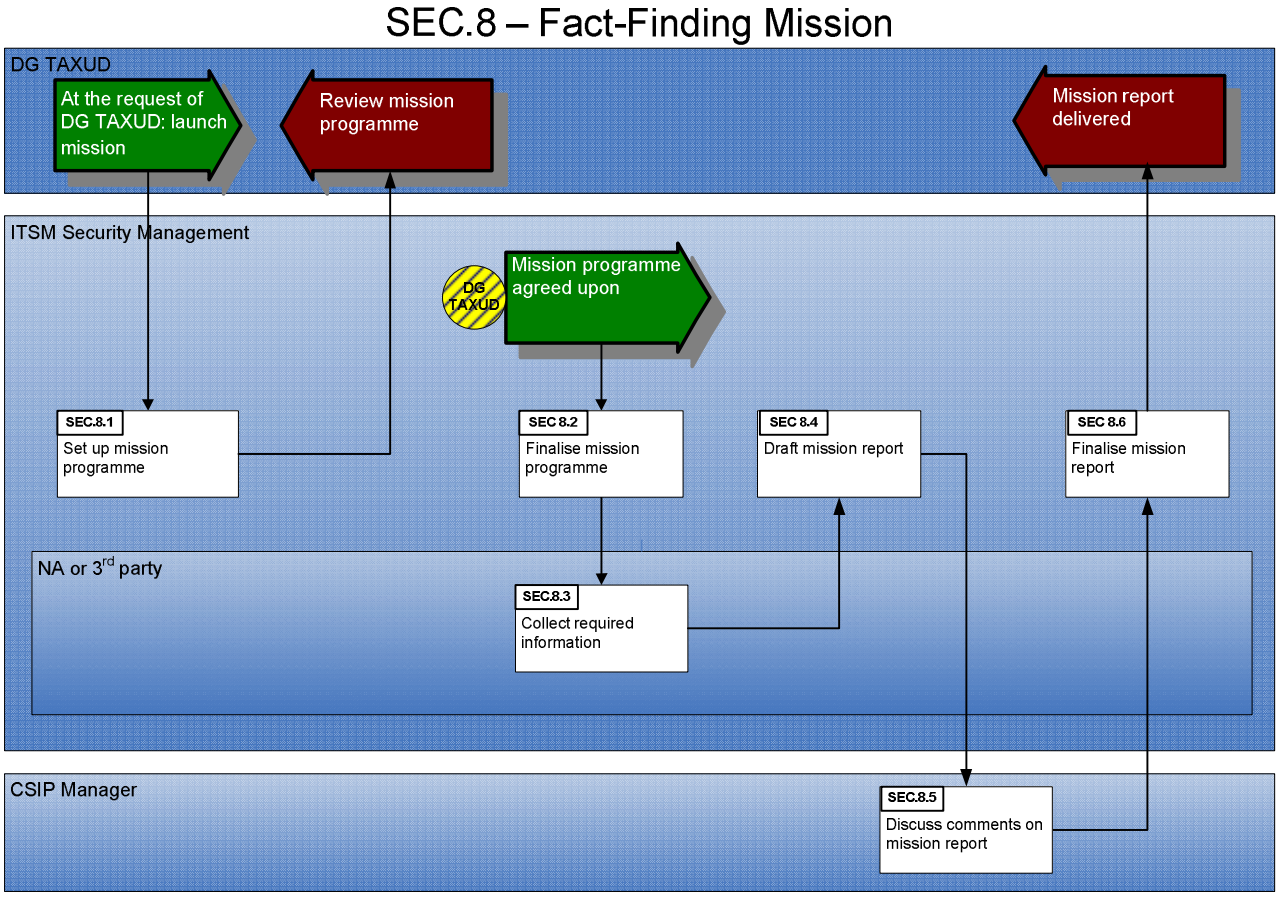

Figure 3: Fact Finding Mission Process

The process starts on request from DG TAXUD. It is executed by ITSM Security Management, who provides the following services:

- Set up of mission programme – At the start of each fact finding mission, the key objectives of the mission are selected. DG TAXUD LISO and ITSM Security Management select which security controls need to be documented during the mission, and which information/ asset need to be provided by the concerned NA or 3rd party during the mission. The selection is based on:
    - Priorities assigned by DG TAXUD LISO;
    - The analysis of security incidents, which originated from the NA or from a 3rd party, and which had an impact on the security of the Common Domain;
    - The results of previous fact-finding missions at the concerned Member States, if any;
    - Changes in policies concerning the Common Domain; changes in trans-European services, if any.

  The result of the set up is a deliverable called "Mission Programme", see §4.4.1 below;
- Collect required information – ITSM Security Management collects the required information through questionnaires and interviews with the concerned NPM (or their representatives) and with their 3rd parties if needed;
- Reporting – See §4.4.2 below;
- Discussion with CSIP – ITSM Security Management discusses the mission report with the CSIP Manager in order to identify possible ITSM service improvements that may help NAs improve their own processes.

A fact-finding mission may include meetings between DG TAXUD and NAs about security; alternatively such meetings may be an outcome of a fact-finding mission. ITSM Security Management provides facilitation services for such meetings. The meeting facilitation service by ITSM Security Management is described in §5 below.

4.3 Roles and Responsibilities

The involved parties are:

- DG TAXUD LISO;
- NAs through the concerned NPMs, who may delegate someone else to represent them;
- 3rd parties of NAs:
    - Services providers such as hosting companies, network service providers, IT management services, or service desk;
    - Suppliers of IT equipment and of software.
- ITSM Security Management;
- ITSM CSIP Manager.

The roles and responsibilities in the frame of the Fact-Finding Mission service are as follows:

Role	Responsibilities
DG TAXUD LISO	• Provide ITSM Security Management with the required information for the set up of the mission programme; • Review/ approve the deliverables.
NPM	The concerned NPMs shall: • Provide required access to information and assets as defined in the mission programme; • Cooperate with DG TAXUD LISO and with ITSM Security Management for the success of the mission • Nominate delegates if needed. The delegates shall have the same authority as the NPM regarding the topics that are addressed in the mission.
ITSM Security Management	• Develop the mission programme; • Collect required information, and provide DG TAXUD LISO with a mission report as described in §4.4.2 below.
ITSM CSIP Manager	• Discuss the ITSM Security Management's mission report; • Identify possible ITSM service improvements that may help NAs improve their own processes for a better security posture.

Table 5: Roles and Responsibilities for fact-finding mission process

4.4 Deliverables

4.4.1 Mission Programme

The Mission Programme is the document ITSM Security Management produces for every fact-finding mission it performs in the frame of the ITSM project. It contains the information that needs to be known before the collection of information can start. The contents are:

- Mission subject – Short description of the objective of the mission;
- Key objectives – Detailed description of the security controls that need to be documented during the mission;
- Scope of mission – Identification of the involved user communities, the involved business threads, and the involved Member States;
- Planning – Identification of contact people; estimate of the workload on concerned people at NAs; identification of information/ assets that need to be provided by the concerned NA during the mission.

4.4.2 Mission Report

The Mission Report is the document ITSM Security Management produces at the end of a fact-finding mission. The contents are:

- Description of mission – Reminder of essential information about the mission (subject, objectives, scope);
- Findings – Findings that are collected during the mission;
- Evidences – Supporting documentation: minutes of interviews, filled questionnaires, other relevant information.

5. Facilitate Meeting

5.1 Scope

ITSM Security Management provides facilitation services for meetings between DG TAXUD and NAs about security.

5.2 Process

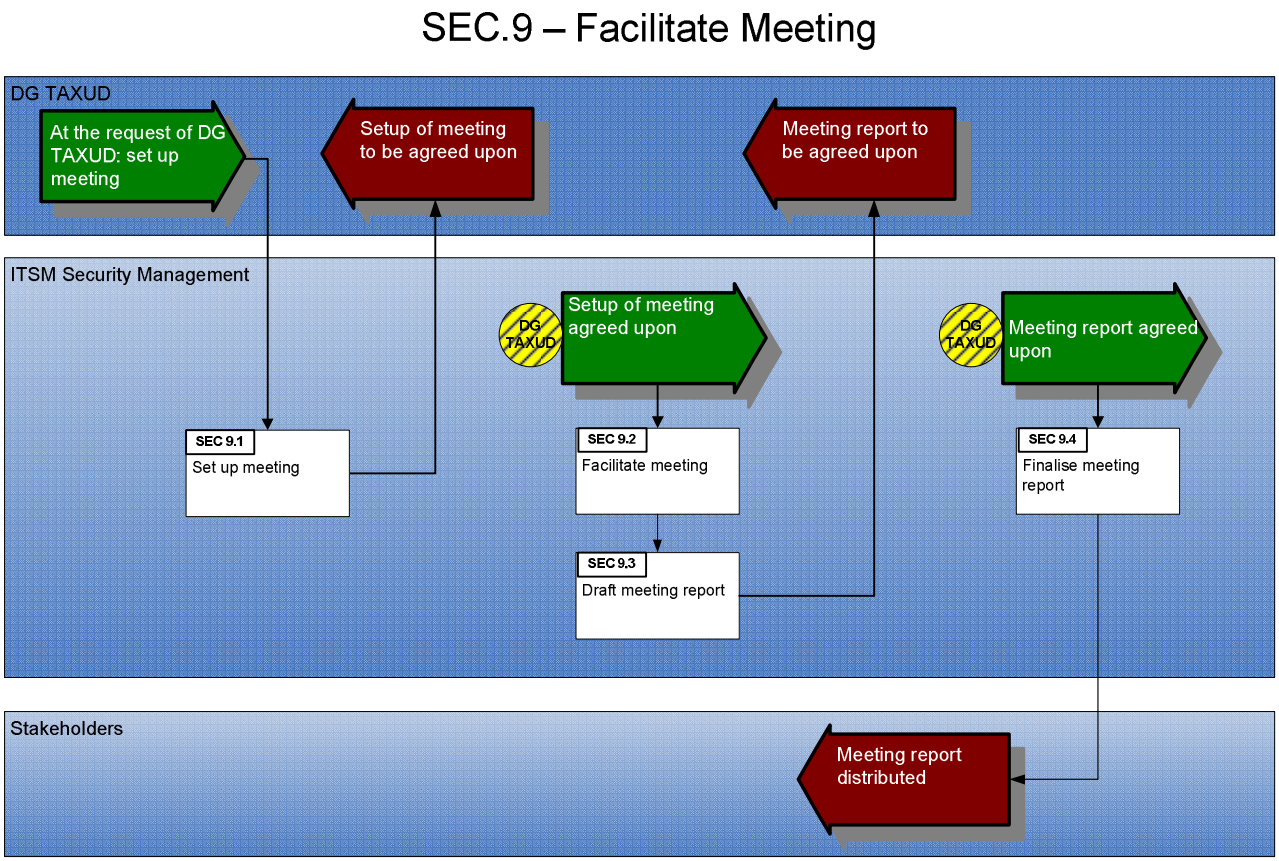

Figure 4: Facilitate Meeting Process

The process starts on request from DG TAXUD. It is executed by ITSM Security Management, who provides the following services:

- Set up meeting – ITSM Security Management agrees with DG TAXUD LISO and NAs NPM about:
  - The agenda;
  - Supporting documents: presentations that need to be done; documents that must be presented during the meeting.

The result of the set up is the "Set up of Meeting" deliverable, which is described in §5.4.1 below. DG TAXUD LISO convenes the meeting by sending the agenda and the supporting documents;

- Facilitate meeting – The meeting is chaired by DG TAXUD LISO. ITSM Security Management services are:
  - Take minutes;
  - Perform presentations if needed;
  - Provide technical expertise to attendees.
- Produce meeting report – See §5.4.2 below.

5.3 Roles and Responsibilities

The involved parties are:

- DG TAXUD LISO;
- NAs through the concerned NPMs, who may delegate someone else to represent them;
- ITSM Security Management.

The roles and responsibilities in the frame of the Facilitate Meeting service are as follows:

Role	Responsibilities
DG TAXUD LISO	• Agree on an agenda; • Convene and chair the meeting; • Review/ approve the deliverables.
NPM	The concerned NPMs shall: • Agree on an agenda; • Participate in the meeting; • Nominate a delegate if needed. The delegate shall have the same authority as the NPM regarding the topics that are addressed in the meeting.
ITSM Security Management	• During meeting: o Take minutes; o Perform presentations if needed; o Provide technical expertise; • Produce deliverables, see §5.4 below.

Table 6: Roles and Responsibilities for "Facilitate Meeting" process

5.4 Deliverables

5.4.1 Set up of Meeting

The contents need to be agreed upon between DG TAXUD LISO, NAs, and ITSM Security Management on a case-by-case basis. Generally the contents are:

- Agenda of meeting;
- If needed: PowerPoint presentations; documents to be presented during the meeting.

5.4.2 Meeting Report

The contents are:

- Review of previous action points;
- Discussed topics;
- New action points.

6. Coordination of Security Incident Management

6.1 Scope

ITSM Security Management coordinates the management of security incidents that occur in NAs and that have an impact on the security of the Common Domain and —possibly— on another NA.

6.2 Process

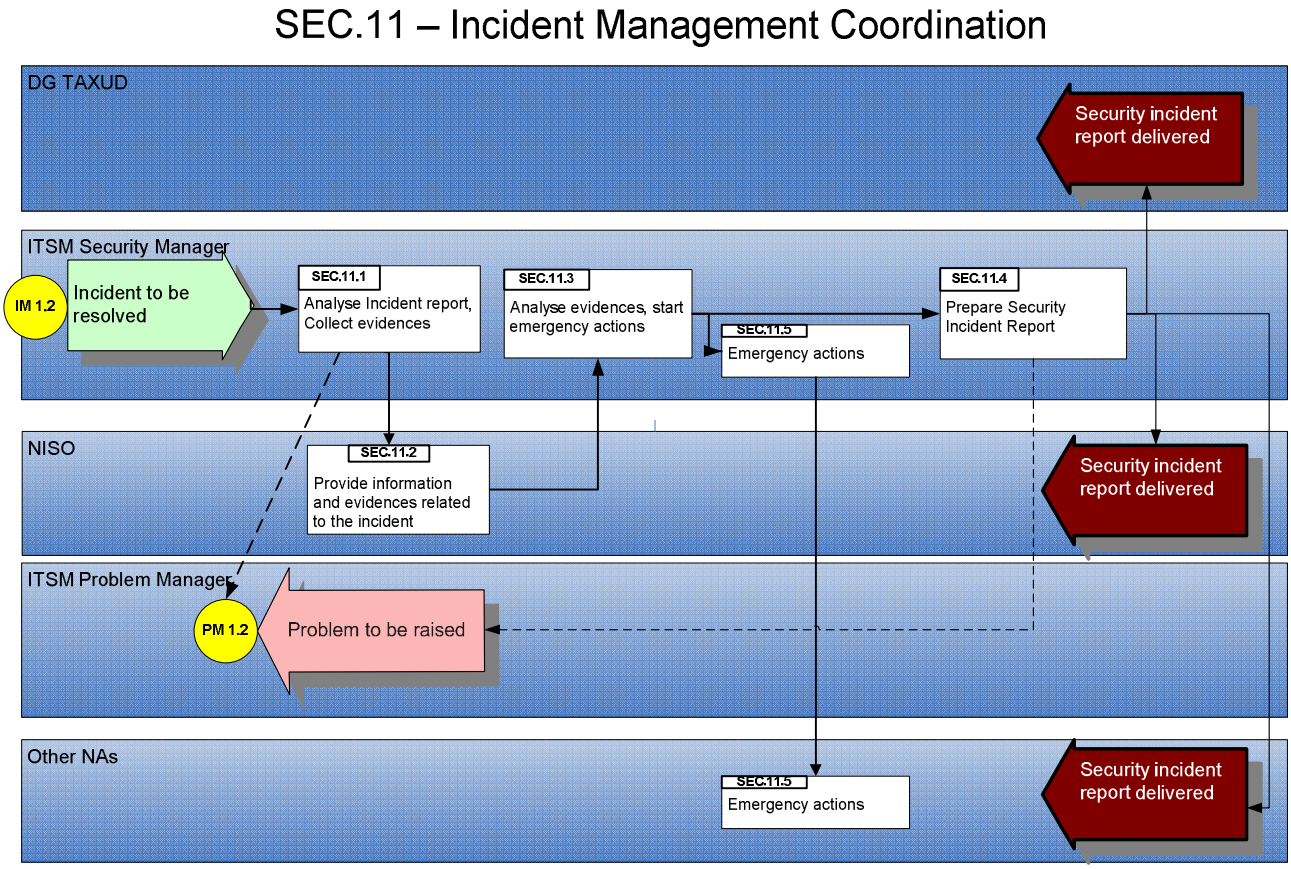

Figure 5: Incident Management Coordination Process

The process is triggered by a security incident that occurs in NAs and that has an impact on the security of the Common Domain and —possibly— on other NAs. ITSM Security Management provides coordination of the following processes:

- Analyse incident report, collect evidences – Upon reception of the security incident from the Incident Management process (see description of the Incident Management

process in applicable document AD2), the ITSM Security Manager analyses the available information as issued by the Service Desk;

- Provide Information and Evidences – The NISO is expected to:
  - Assist in investigating the incident;
  - Provide information on the incident;
  - Gather technical evidences contained in the systems and/or applications logs.
- Analyse Evidences – Based on the information compiled by the NISO, the ITSM Security Manager analyses the evidences and checks them for consistency;
- Emergency actions – When required ITSM Security Manager sends requests for emergency actions and distributes them
  - Across the ITSM organisation to the appropriate Security Officers who will be responsible to perform those actions;
  - To the NISOs in the concerned NAs. If a security incident is detected in one NA, with impact on another NA, the NISO has to liaise with the other NISO directly, to take emergency actions.

  Requests for emergency actions are detailed by system, impact and urgency;
- As mentioned in Annex 12 of applicable document [AD2], "all incidents concerning Capacity Management, Installations, CCN configuration, as well as incidents for the managed configuration items where the SD cannot provide a solution within 2 hours are assigned to Application Management";
- If the security incident is considered as "high impact" (i.e., the incident had a significant impact on the availability or on the integrity of TAXUD information systems that DG TAXUD classifies as "critical" or "strategic", or an impact on the confidentiality or on the integrity of TAXUD information that DG TAXUD classifies as "limited"), ITSM Secuirty Management.prepares a Security Incident Report – See §6.4.1 below
- Deliver Security Incident Report – ITSM Security Management delivers the Security Incident Report to DG TAXUD LISO, to the NISO and (when needed) to other NAs that may be impacted by the Security Incident.

6.3 Roles and Responsibilities

The involved parties are:

- The NA where the incident occurred, through a NISO;
- ITSM Security Management.

The roles and responsibilities in the frame of the Coordination of Security Incident Management service are as follows:

Role	Responsibilities

NISO	• Provide information and evidence related to the incident; • Perform emergency actions when required.
ITSM Security Management	• Coordinate incident management: collection, analysis, reporting; • Produce deliverables, see §5.4 above.
ITSM Security Officer	• Perform emergency actions when required.

Table 7: Roles and Responsibilities for Security Incident process

6.4 Deliverables

6.4.1 Security Incident Report

For each security incident that is considered as “high impact”, the development of a Security Incident Report is coordinated by ITSM Security Management (security incidents that are not considered as “high impact” do not lead to a Security Incident Report, e.g., an unsuccessful virus attack; nevertheless ITSM Security Management launches emergency actions when needed by a security incident that is not considered as “high impact”, see description in §6.2 above). A Security Incident Report traces back the root causes of the incidents, the chain of events leading to the security incident, the related issues, the lessons learned and the actions taken. The report is presented to the DG TAXUD LISO for information.

The structure of the document is the following:

1. Management Summary
2. Security Incident Short Description
   - 2.1 Identification
   - 2.2 Overview
   - 2.3 Parties Involved
   - 2.4 Customer Services Affected
3. Security Incident Analysis
   - 3.1 Analysis of e-mail exchanges related to incident
   - 3.2 Log File Analysis / Identification of origin
   - 3.3 Chain of Events
     - 3.3.1 Detection
     - 3.3.2 Registration
     - 3.3.3 Resolution
     - 3.3.4 Recovery
     - 3.3.5 Closure

3.4 Gap Analysis 3.4.1 Analyse any deviation from security policy the incident could reveal 4. Recommendations

Table 8: Security Incident Report Structure