OWNER:	ISSUE DATE:	VERSION:
DG TAXUD	22/03/2010	1.04

TAXATION AND CUSTOMS UNION DG
ITSM

SUBJECT:

FQP - Annex 12: Incident Management

FRAMEWORK CONTRACT # TAXUD/2007/CC/088

Document History

Edi.	Rev.	Date	Description	Action (*)	Pages
0	01	06/07/2007	First Draft	I	All
0	02	05/10/2007	Further implementation	I/R	As req.
0	03	08/10/2007	Further implementation	I/R	As req.
0	04	15/10/2007	Draft delivered for information to DG TAXUD	I/R	As req.
0	05	31/10/2007	Draft delivered for information to DG TAXUD	I/R	As req.
0	06	30/11/2007	Further implementation + Implementation of comments received from DG TAXUD. Delivered for information to DG TAXUD	I/R	As req.
0	07	10/12/2007	Further updates	I/R	As req.
0	08	01/04/2008	Further updates	I/R	As req.
0	09	07/07/2008	Consolidation after intermediate deliveries of processes outside of the scope of the FQP document	I/R	As req.
0	10	15/07/2008	Delivered for review to DG TAXUD after internal QC	I/R	As req.
1	00	07/11/2008	Delivered for acceptance to DG TAXUD after implementation of review comments	I/R	As req.
1	01	28/11/2008	Re-delivered for acceptance to DG TAXUD after implementation of remaining comments	I/R	As req.
1	01-2	05/10/2009	First evolutive version	I/R	As req.
1	01-3	20/10/2009	Further updates version	I/R	As req.
1	01-4	10/11/2009	Further updates version	I/R	As req.
1	01-5	24/11/2009	Further updates version	I/R	As req.
1	01-6	01/12/2009	Further updates version	I/R	As req.
1	01-7	07/12/2009	Further updates version	I/R	As req.
1	01-8	08/12/2009	Sent for internal review and implementation of QC comments	I/R	As req.
1	01-9	10/12/2009	Sent for information to DG TAXUD	I/R	As req.
1	01-10	15/01/2010	Updated with CCO	I/R	As req.

1	02	01/02/2010	Delivered for review to DG TAXUD after internal QC	I/R	As req.
1	03	05/02/2010	Re-delivered for review to DG TAXUD after internal QC	I/R	As req.
1	04	22/03/2010	Delivered for acceptance to DG TAXUD	I/R	As req.

(*) Action: I = Insert R = Replace

Table of Contents

List of Tables

List of Figures

1. Introduction

This document is an annex to the Framework Quality Plan, deliverable DLV 0.1.1 requested in Specific Contract 04 [A2] under Framework Contract (IT Service Management for DG Taxation and Customs Union) [A1], Work Package WP.0.1.

This document presents the Level 1, 2 and 3 of the ITSM process FQP - Annex 12: Incident Management.

2. Reference and Applicable Documents

This chapter presents two lists of relevant programme related documents. They are divided into reference and applicable documents.

2.1 Reference Documents

Id	Reference	Title	Date	Version
R1	ITS-IFQP-SC04-Framework Quality Plan	Framework Quality Plan	22/03/2010	1.04
R2	ITS-IFQP-SC04-Annex 9	ITSM Glossary	22/03/2010	1.13

Table 1 – Reference documents

2.2 Applicable Documents

An applicable document is a document which content is binding for a contractor no matter what is mentioned in this FQP.

Id	Reference	Title	Date	Version
A1	TAXUD/2007/CC/088	Framework Contract	04/05/2007	N/A
A2	TAXUD/2008/DE/114	Specific Contract 04	30/06/2008	N/A
A3	QAC-SC01-FQP_TEM	Framework Quality Plan Template	N/A	1.01

Table 2 – Applicable documents

3. Terminology

3.1 Abbreviations and Acronyms

A list of the abbreviations and acronyms used in the context of the ITSM Programme, and more specifically for this document is provided in Annex 9 ITSM Glossary [R2].

3.2 Interface with DG TAXUD

Where there is a non-specific reference to DG TAXUD, Directorate Generale Taxation and Customs Union DG or other similar descriptions, it means that the interface can be with any one of the following business threads of DG TAXUD:

- DG TAXUD A4/CPT,
- DG TAXUD A4/ISD,
- DG TAXUD A4/APM
- DG TAXUD A3/TAX,
- DG TAXUD A3/EXC,
- DG TAXUD A3/CUST,
- DG TAXUD A3/LISO.

Where it is intended that a reference is to a specific business thread, one of the business threads above shall be stated.

4. ITSM Process model

4.1 Level 0: Process flows

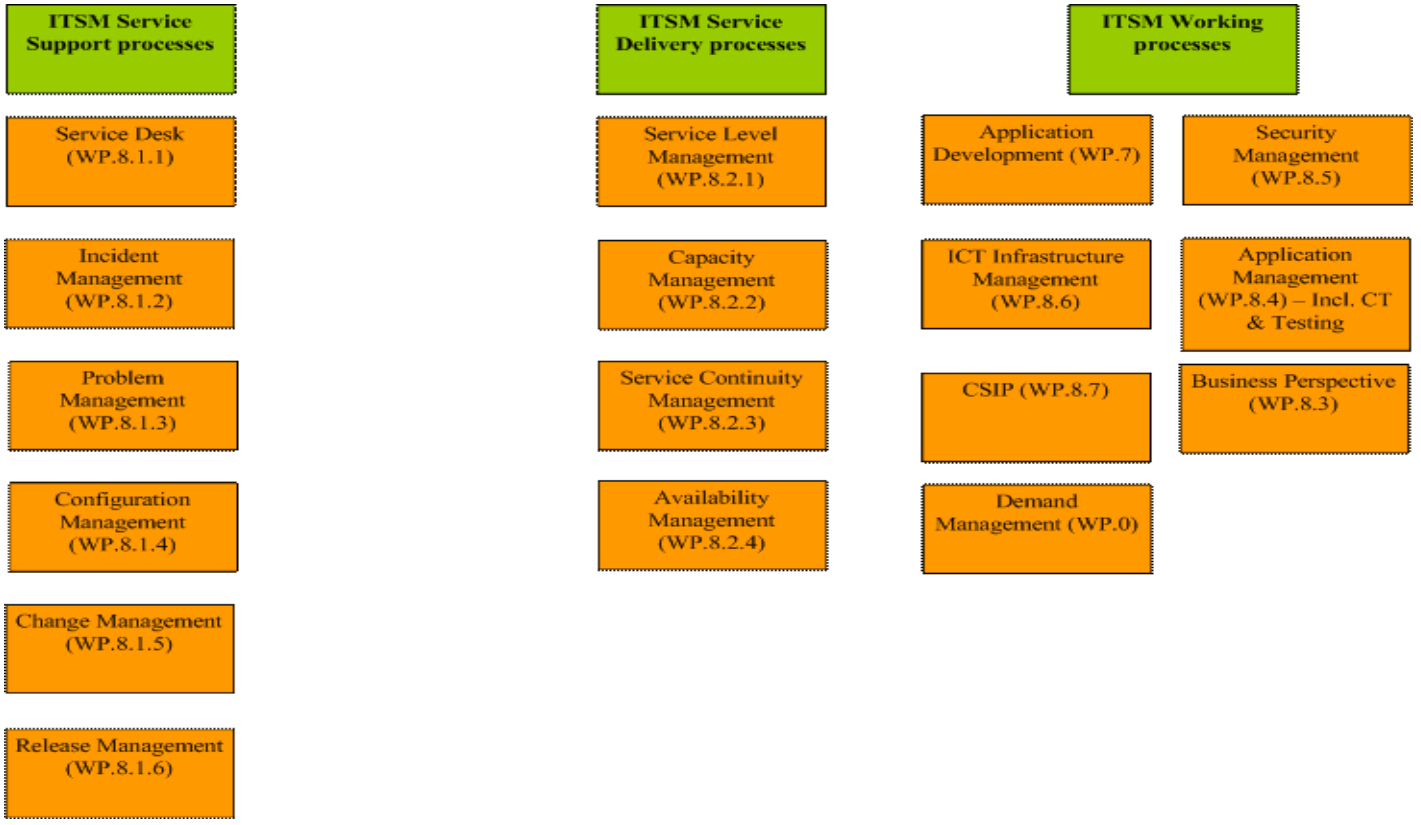

Figure 4-1: ITSM Process Model

4.2 Level 1: Incident Management

The goal of Incident Management is to restore normal service operation as quickly as possible and minimise the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

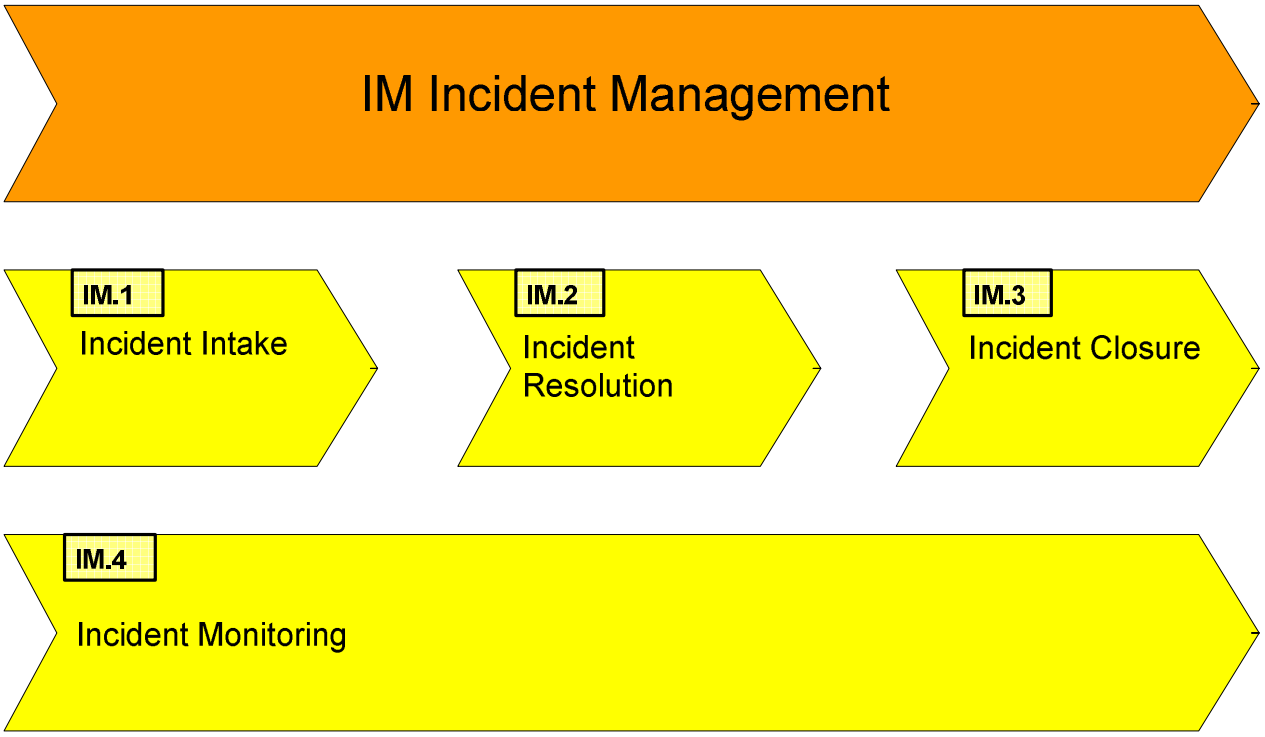

Figure 4-2: IM Incident Management sub-processes

4.3 Level 2: Incident Management

IM.1 Incident Intake

This step covers the acknowledgement, registration and assignment of an incident.

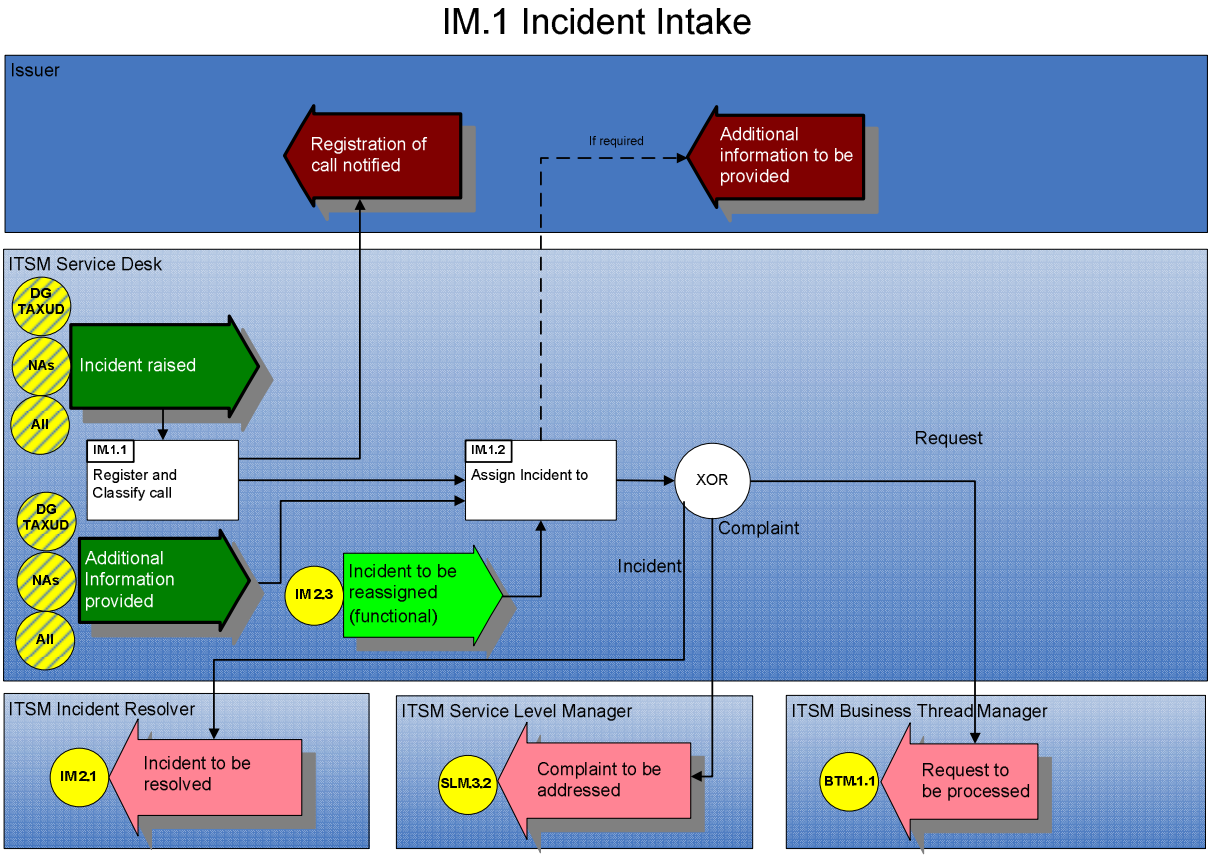

Figure 4-3: IM.1 Incident Intake

IM.2 Incident Resolution

This step presents how is handled the resolution of an incident.

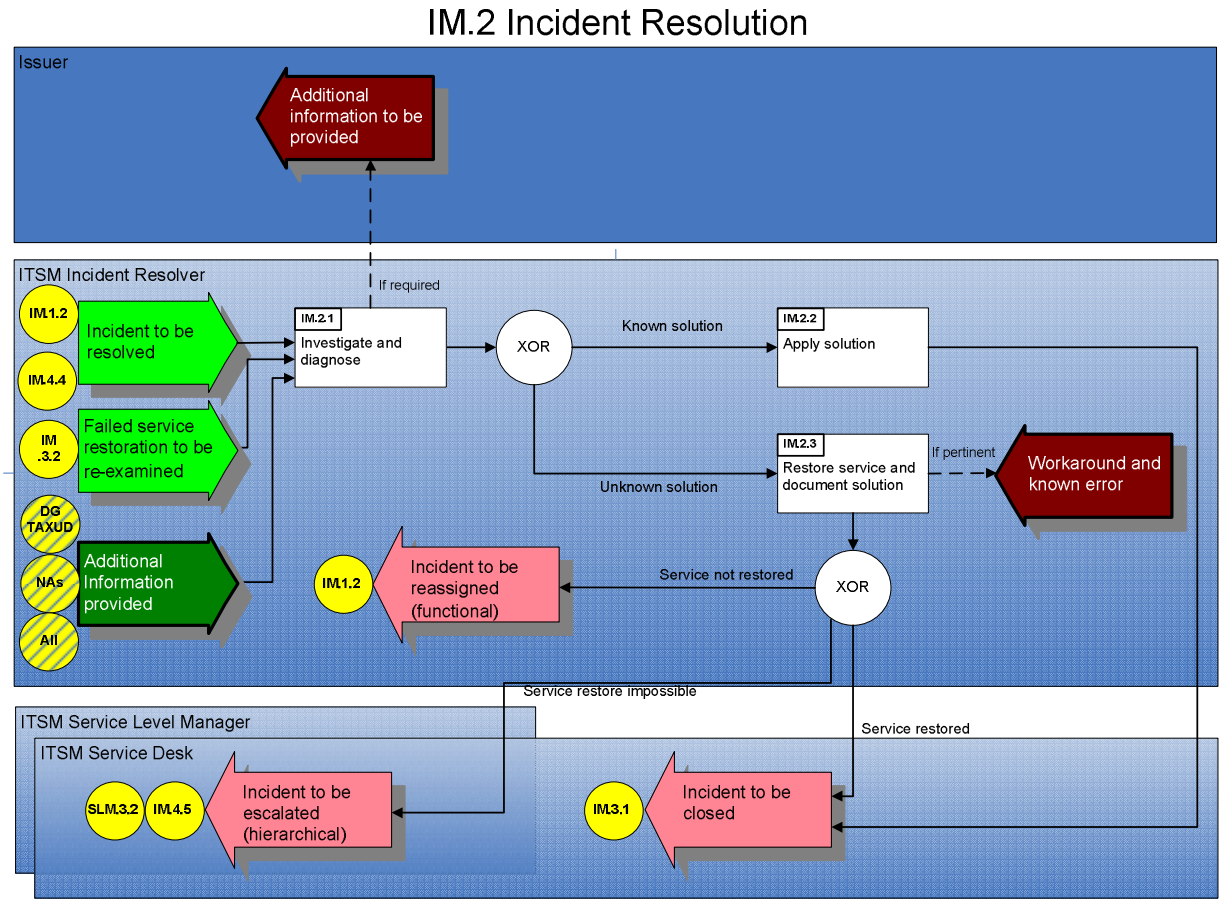

Figure 4-4: IM.2 Incident Resolution

IM.3 Incident Closure

This step presents the closure of an incident[1].

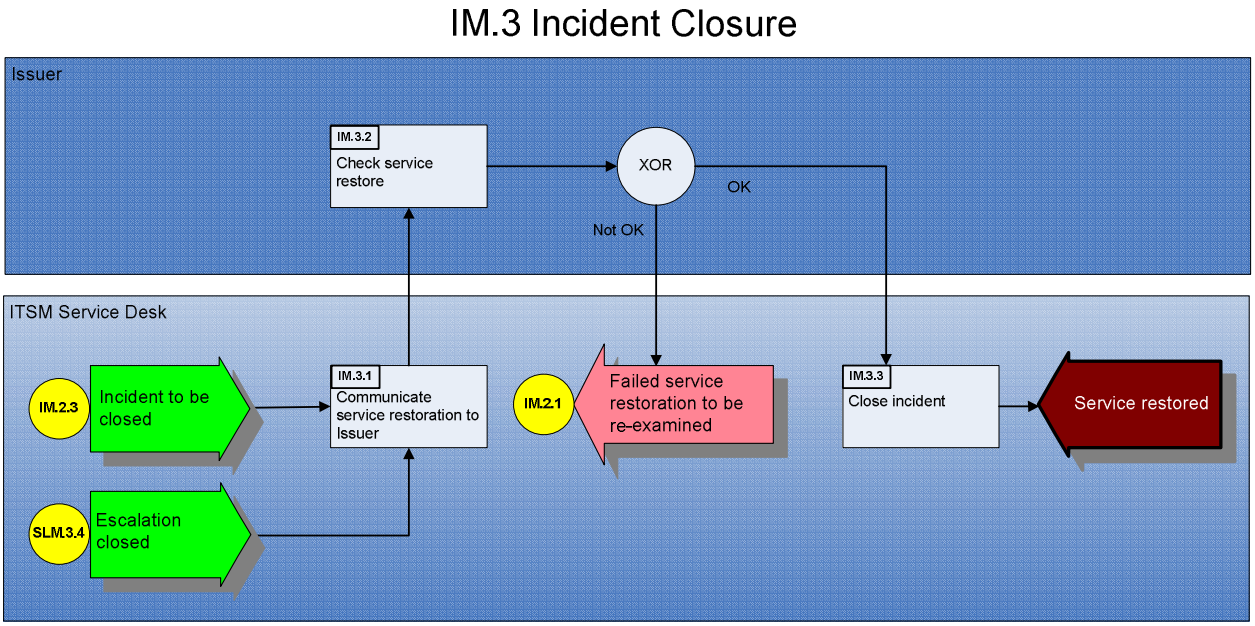

Figure 4-5: IM.3 Incident Closure

[1] Please note that Box 4.2 is not visible in the Incident Closure figure as:
- IM 4.2 generates a reminder when the Service Call is solved and can be closed and the user did not acknowledge the first closure request (IM 3.2);
- IM 3 is the standard close procedure and never issues a reminder - it just checks service restoration (IM 3.2)

IM.4 Incident Monitoring

This step presents how is monitored an incident throughout its lifecycle.

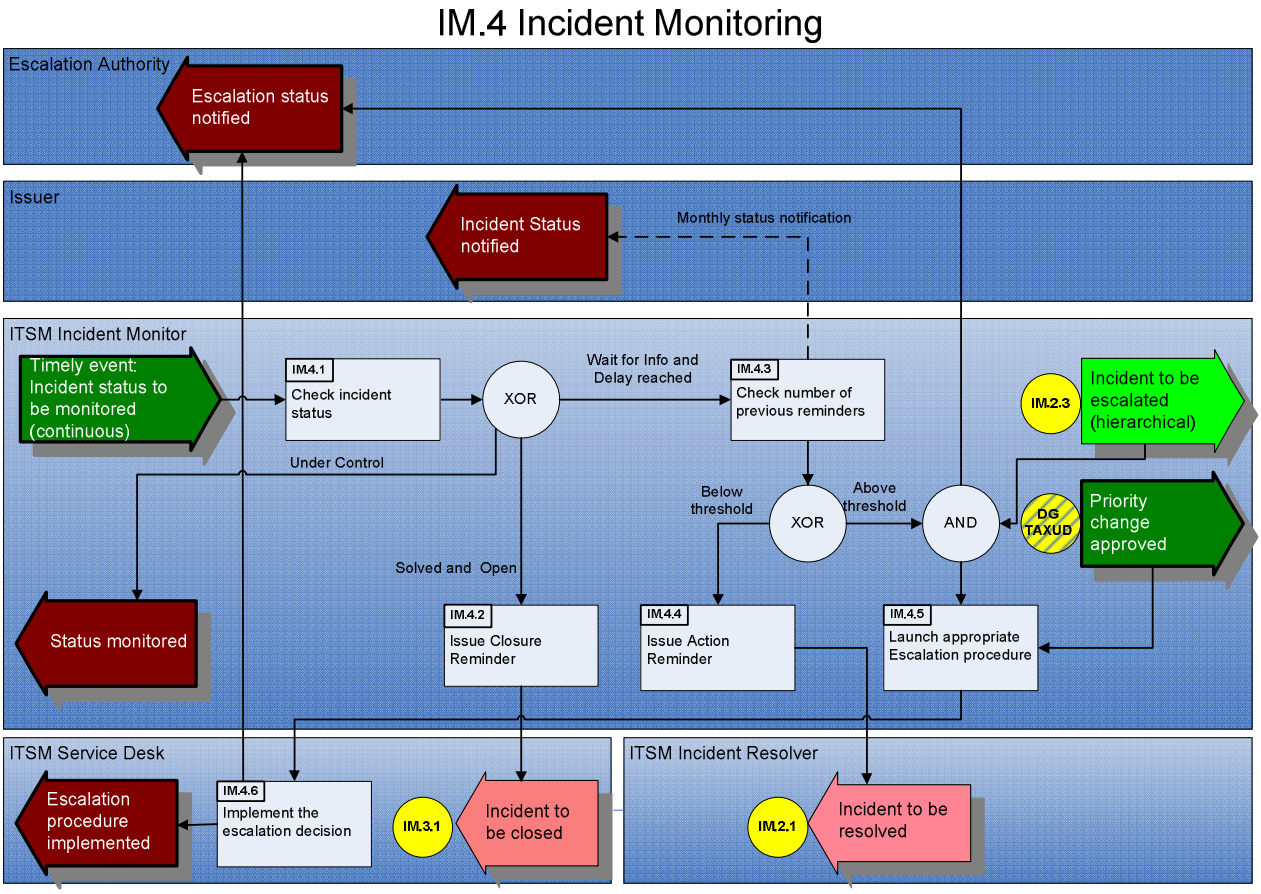

Figure 4-6: IM.4 Incident Monitoring

RACI Table for IM

Activity	Issuer	ITSM Service Desk	ITSM Incident Resolver	ITSM Demand Manager	ITSM Service Level Manager	ITSM Problem Manager	ITSM Incident Monitor	Escalation Authority	DG TAXUD A4/CPT	DG TAXUD A4/ISD	DG TAXUD A4/APM	DG TAXUD A3/Tax	DG TAXUD A3/Exc	DG TAXUD A3/Cust	DG TAXUD A3/LISO
IM.1.1 Incident Intake	I	RA					I		I	I	I	I	I	I	I
IM.1.2 Incident Resolution		I	RA	I	I		I		I	I	CI	CI	CI	CI	CI
IM.2.1 Investigate and Diagnose		I	RA				I		I	I	CI	CI	CI	CI	CI
IM.2.2 Apply solution		I	RA				I		I	I	CI	CI	CI	CI	CI
IM.2.3 Restore Service and document solution		I	RA		CI	CI	I		I	I	I	I	I	I	I
IM.3.1 Communicate Service Restoration to issuer	I	RA					I		I	I	CI	CI	CI	CI	CI
IM.3.2 Check service restore	RA	I							I	I	CI	CI	CI	CI	CI
IM.3.3 Close Incident	I	RA					I		CI	CI	CI	CI	CI	CI	CI
IM.4.1 Check Incident status	I						RA		I	I	I	I	I	I	I
IM.4.2 Issue Closure reminder		I					RA		I	I	I	I	I	I	I
IM.4.3 Check number of previous reminders							RA		I	I	I	I	I	I	I
IM.4.4 Issue action reminder			I				RA		I	I	I	I	I	I	I
IM.4.5 Launch appropriate escalation procedure	I	I	I		I		RA	CI	CI	CI	CI	CI	CI	CI	CI
IM.4.6 Implement the escalation decision	CI	RA	CI		CI		I	CI	CI	CI	CI	CI	CI	CI	CI

Table 4-1: IM RACI Table

Communication interfaces with DG TAXUD

Interface description communication with DG Taxation and Customs Union	Direction	Format
IM.1.1 Incident Intake		
DG TAXUD contact with SD	Incoming	Email, Phone, Fax, PST, Letter, Web page, communicator
Acknowledge	Outgoing	Email
Request for Information	Outgoing	Email
IM.2.1 Investigate and Diagnose		
assign incident (internal)	Outgoing	Mail, Phone, update internal SD tool
assign incident (DIGIT)	Outgoing	IRMA
assign incident (other third party)	Outgoing	Email, Phone, task assigned via SD Tool. Visible on the ITSM Portal
Request for Information	Outgoing	Mail, Phone
IM.2.3 Restore Service and document solution		
Inform of problem	Outgoing	Email
IM.3.1 Communicate Service Restoration to issuer		
Inform Issuer of resolution	Outgoing	Email, Phone, task assigned via SD Tool. Visible on the ITSM Portal
IM.3.2 Check service restore		
Inform of working resolution	Incoming	Email
IM.3.3 Close Incident		
Inform Issuer restoration of service	Outgoing	Email, Phone
IM.4.5 Launch appropriate escalation procedure		
Escalation if done by DG Taxation and Customs Union	Incoming	Email, Phone
Escalation information if done by ITSM	Outgoing	Email, Phone
IM.4.6 Implement the escalation decision		
Communication of escalation procedure	Outgoing	Email, Phone

Table 4-2: IM Communication interfaces with DG TAXUD

4.4 Level 3: Incident Management

Procedure	
IM.1.1 Register and Classify Incident	**IM.1 Incident Intake** **IM.1.1 Register and Classify Incident** Any received request, being an incident (failure), a Service Request or a complaint, is registered by the SD as an incident in the ITSM SMT. The registration requires the accomplishment of two activities, the *registration* activity and the *classification* activity, as described below. During the registration and classification activity, the following tasks are accomplished: • Assign the incident ID: a unique number for each incident; • Assign a Business Thread, Configuration Item and set the Security flag; • Give the incident Name: a title for the incident, usually derived from the subject of the original incoming e-mail or from the content of the request (when the actual e-mail subject is not a clear description of the request); • Set the time stamp of the received e-mail, fax or letter in the reception time field; • Assign the incident category; • Assign the Priority level; • Choose the relevant environment of the incident, i.e. “OPER", "CONF", "SAT", "PRE-SAT”; • Indicate whether the incident is externally visible or internal to ITSM. Internal incidents are opened for issues that need to be handled within ITSM and implicate internal activities from the different stakeholders of ITSM. Internal incidents are set to 'internal' and are therefore not visible on the ITSM portal. During the logging of an incident, the SDO enters the following information at the incident level: *Italics: automatically filled fields*, **bold:** mandatory fields **Incident Attributes** **Fields** — **Content** *Incident ID* — Unique number assigned to an incident with the format: INCyymm.xxxxx (automatic by the system), where yy are the last two digits of the current year, mm the current month, and xxxx a serial number. **Business Thread** — The Business Thread associated with the Incident **Incident Category** — The incident category as described in table 7-4. Configuration Item — The Configuration Item to which the Incident refers Security Flag — Whether the incident is a security issue (yes/no) **Incident Name** — The Subject of the original e-mail or a short description if the request comes by phone call or when the description provided by the SD User is not at all

representative for the request.

User Management The name of the issuer or *requester* of the incident.

If the user is a person, the organisation is also entered, if the user is an organisation with a generic e-mail address then the requester name remains blank.

Reception time The time the original e-mail, fax or phone came.

Registration time The time the incident is registered into the ITSM SMT (automatically given by the system).

Reception mode This may be: e-mail, phone, fax, and letter.

Environment Specifies the environment where the problem occurred. The following environments are available: OPER, CONF, SAT, PRE-SAT.

Status This can be one of the following values: "Open", "Assigned Internal", "Assigned External", "Wait for Info", "Wait for SOL", or "Closed"; the *initial status is "Open" during the creation and registration.*

Table 4-3: Incident Attributes in ITSM SMT

The SD registers incidents and classifies them into one of the following four main *categories*:

Category	Description
Incident or Failure	Relates to failures or deviation from expected behaviour in software, connectivity, performance, application configuration, operations, capacity or connection problems, for the managed configuration items.
Service Request	Relates to handling of organisational questions and requests for documentation, publications, business information, User Management, management and delivery of translations, organisation of conference calls/virtual meetings, remote/on site technical support, ad hoc support, training management, qualification, Conformance Testing, testing of full release, installation, management notifications of scheduled or unscheduled unavailability and requests for mass e-mails.
Complaint	All complaints, i.e. negative information about the quality of the service received from the authorised SD users are registered in the ITSM SMT. The official complaints received by letter from DG TAXUD are not registered here.
Request for Information	All requests received on technical, applicative or business aspects of the managed configuration items and associated documentation.

Table 4-4: Incident Categories

Any registered event of the Service Desk is called an incident. This includes both 'incidents' in the sense of failures, and Service Requests. When requests and complaints are addressed, they are mentioned explicitly. After the incident is registered, the SD decides whether this remains an incident where a

restoration of a failure is needed, or whether the received incident is a Service Request, being handed over to the Demand Management process.

The Service Catalogue Request is a form that triggers the order of one of the following requests: ad hoc support, meeting room request, conference call, remote support, documentation, on-site support, translation or training. The SD receives Requests for Service Catalogue elements automatically from the ITSM portal. These requests are logged in the ITSM SMT and handled by the SD as external incidents.

A list of managed configuration items, along with the related documentation and information from requestor is used by the SD for identifying the context of an opened incident.

Incident Priorities

Incidents are classified according to their priority levels. These are taken from each thread according to the respective SLA. The priority of an incident is an integer between 1 and 4:

- 1: Critical;
- 2: High;
- 3: Medium;
- 4: Low.

The priority is calculated from two other parameters: the impact and the urgency.

Priority/Resolution times calculation table from urgency and impact

Impact	Low		Medium		High	
	Priority	Res.T.	Priority	Resp.T.	Priority	Res.T.
Urgency						
Low	4	65h	3	39h	2	13h
Medium	3	39h	2	13h	1	4h
High	2	13h	1	4h	1	4h

Table 4-5: Priority/Resolution times calculation table

Impact definition table

	Impact Definition Low Independent users reporting incidents or requesting services from the SD. Medium One NA experiencing problems with the managed configuration items without affecting other NAs. High More than one NA reporting problems on the managed configuration items or one NA that can affect others as well. Table 4-6: Impact Definition table **Urgency definition table** **Urgency Definition** • Low Inquiries on technical, applicative or business aspects of the managed configuration items and associated documentation; • Minor functions of the managed configuration items does not work as specified but this doesn't prevent the end users or the NAs of using them; • Non Blocking issues on the Configuration Items; • Issues with SAT/PRE-SAT; • Messages rejected between countries; Dead Letter Queues. • Medium One application or one server down; • Major functions of the managed configuration items does not work as specified; • Capacity issues; • Requests for Web updates; • User Right Management Requests; • Conference calls; • Hotfix issues in PRE-SAT/SAT; Incidents occurring within Mode 2 CT campaigns • High Blocking incidents of the Configuration Items; • DDS public website down; • Entire domain down; • Transmission of corrupted data; • Confidential information could be divulged and affect the interest of EU or its civil servants; • Incidents that can result to financial suffer prejudice of the Commission or other parties; Notifications of unscheduled unavailability. Table 4-7: Urgency Definition table The SDOs choose the impact and urgency according to the two tables (Table 4-6 and Table 4-7) and the ITSM SMT then automatically calculates the priority of the incident. If the issuer

disagrees with priority, he/she can escalate through IM.4.5.

The priority levels of an incident determine the allowed solution time, the frequency of reminders and the additional persons that need to be notified in case a Critical priority incident.
The *resolution time* is the time interval (working hours) after the incident registration in which a solution must be sent to the issuer.
The *response time*, that is maximum time interval (working hours) that is allowed passing between the reception of an event and the closing of the first action (acknowledgement action).

The resolution time of the incidents according to their priority level and the thread are presented in the tables below:

	Response time (ACK)	**Solution time**			
		Low	Medium	High	Critical
In hours	1h	65h	39h	13h	4h

Table 4-8: Response times and resolution times according to SLAs

The first action the SD performs after recording, is to send an acknowledgement e-mail (ACK e-mail) informing the SD User (or *requester*) that his/her request has been received and properly registered. This ACK e-mail includes the incident ID and the request to the issuer to include this incident ID in the subject of all communication to the SD.

The incident registration and the sending of the acknowledgement must be accomplished within one hour from the reception of the e-mail, phone call or fax.

For the first action, the sending of the ACK e-mail, and for any consecutive action, the SDO fills the following fields into the ITSM SMT in the action level that is below the incident level:

Italics: automatically filled fields, **bold**: mandatory

Action attributes

Fields	**Content**
Action ID	Unique number assigned to an action with the format: INCyymmxxxxx. n were n is the number of each action (automatic by the system) and where yy are the last two digits of the current year, mm the current month, and xxxx a serial number.
Creation Time	The date and time the action is registered into the SD database (automatic by the system).
Name	The brief sentence from the first step above, describing the action expected by the assignee of the action e.g. Please provide your position, please provide

	requested Information, Please deliver ..., Please Investigate, …. **Impact** The Impact definition of the incident:: High, Medium, Low, that together with Urgency definition, automatically calculate the priority **Urgency** The Urgency definition of the incident:: High, Medium, Low, that together with Impact definition automatically calculate the priority *Priority* The severity level of the incident: 1: Critical, 2: High, 3: Medium, 4: Low, that determines the resolution time. (automatic by the system). The priority is derived from a combination of Impact and Urgency. Suggested Solution Detailed description of the current action. The exchanged e-mails that provide the solution to any action. For the first action, the ACK e-mail is attached in this field. *Closure time* The time the action closes (automatic by the system). *SD Operator* The Service Desk Operator registering this action. **Assigned to** Specifies the name of the ITSM party or the external to ITSM party that is responsible for providing the resolution of the incident at a given action or handling the information received. **Status** Indicates the current status of an incident (open,Wait fir Info, Assigned internal/external, Solved, Wait for Solution ...) Table 4-9: Action Attributes in ITSM SMT

IM.1.2
Assign Incident to

IM.1.2 Assign Incident to Incident Initial investigation- Assignment Procedure

After the ACK e-mail has been sent, the second action is created. Therefore, the SDO decides whether the SD solves the incident or whether additional information is required prior to solution, or whether the incident needs to be assigned to another party outside the SD for action, approval or solution. The SDO sets the status of the incident from the initial 'Open' status to one of the following statuses: *Wait for Info, Assigned Internal or Assigned External"*

Wait for Info: If additional information is needed, the SDO creates an action in the ITSM SMT and sets the status of both action and incident to "*Wait for Info"*. This status is needed to indicate that the solution has been suspended because some additional information is necessary. This action is always assigned to the SD User who has to provide the requested information. The Action Name field of this action is filled in with a short description of what is expected by the SD User, e.g.: "Please provide requested information", or "Please send us your feedback" etc. The e-mail with the details of the requested Info is attached to the Description field. The whole incident is also set to status "*Wait for Info*", in agreement with the action status.

Every incident that is assigned to DG TAXUD for resolution is always set to status "*Wait for Info*" and the assignee is the concerned DG TAXUD's department.

When the requested information arrives, the SD attaches the received e-mail in the Suggested solution field and closes the action. The possible status transitions are now: Assigned Internal, Assigned External or Wait for Info

Assigned Internal: If the SDO decides that no additional information is needed for the solution, the incident is assigned for solution to the resolver. If the resolver is the SD, or another internal ITSM party, then the action is set to the status *"Assigned Internal"* and similarly to the rationale of filling the action name field of the previous *"Wait for Info"* step, the action name is set to a short action description. The name of the solution party where this incident is assigned for solution is set in the resolver field. If the resolver is not the SD then an e-mail with the details of the action expected from the other party is sent. This e-mail is inserted in the Description field of this action including the e-mail header that includes recipients, and time stamp.

Assigned Ext. Similarly to the *"Assigned Internal"* status above, if the resolver is external to ITSM (like EMCS/DEV CUST/DEV…) then the action and the incident is set to *"Assigned External"*. The Action e-mail sent to this party includes the details of the action expected by that party, and this e-mail is entered in the description field of the action, including the e-mail header that includes recipients, and time stamp. The subject of the assignment e-mail includes the action number within the incident that is assigned to the team.

If the incident is a Service Request, it is assigned to the ITSM Business Thread Manager who makes the follow-up on it (see BTM Management process).

If the incident is a complaint, it is assigned to the ITSM Service Level Manager (see SLM process).

Assignment Rules

The SD is the assignee for the following requests:

- Publications;
- User management;
- Mailing list updates;
- Information to the concerned users about any scheduled or unscheduled unavailability of the applications;
- Mass e-mails.

All the mass e-mails that are disseminated by the SD are in English with the exception of the Customs Business Thread for which ... has retained the trilingual format from the previous contractor. All mass mails are handled by the ITSM SD itself.

Assignment Rules where the ITSM AM is the assignee:

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 and the status of both the "Action" and the "Incident" is set to "*Assigned Internal*". The Assignee in this case is ITSM AM.

In case of incidents concerning problems or inquiries on the behaviour of the managed configuration items in the Conformance environment during the time where the NAs are testing on their own initiative, they are recorded under the category "Incidents" and are assigned either to ITSM Application Management or to ITSM SD for solution. These do not belong to any testing category. The testing categories are reserved for the planning and performance of tests, not to solve incidents in testing environments.

Assignment Rules where the ITSM Infrastructure is the assignee:

All incidents concerning requests, user account management for any ITSM Tools, COTS and mailing list management are assigned to ITSM Infrastructure team (Note: Mailing list updates can also be done by the Service Desk). The status of the "Action" as well as the "Incident" is set to *"Assigned Internal"*. The assignee in this case is ITSM Infrastructure.

Assignment Rules where the ITSM Business Monitoring is the assignee:

All incidents concerning requests for purging the CCN DeadLetter Queues of an NA are assigned to ITSM Business Monitoring. The status of the "Action" as well as the "Incident" is set to "*Assigned Internal*". The assignee in this case is ITSM Business Monitoring.

Assignment Rules where an external to ITSM party is the assignee:

Incidents that concern Database administration and Unix environment administration (where ITSM does not have the privileges to perform necessary actions), Software installations of Oracle clients or Web logic, instances, as well as VPN connectivity problems, that ITSM experiences, coming from DG TAXUD' side are assigned to DIGIT Data Centre.

The status of the "Action", as well as the "Incident" is set to *"Assigned External"* and the assignee is DIGIT. Incidents that concern CCN configurations or trouble incidents for the CCN Queues of the commission are assigned to CCN/TC and the status of the "Action", as well as the "Incident" is set to *"Assigned External"*. The Assignee in this case is CCN/TC.

Incidents that concern CCN configurations or trouble incidents for the CCN Queues of the NAs (e.g. rejection of messages sent between NAs) are assigned to the NAs. The status of the action as well as the incident is set to *"Assigned External"*. The Assignee in this case is the concerned NA.

IM.2 Incident Resolution

IM.2.1 Investigation and Diagnosis

Depending on the first investigation of the SDO, the incident is

IM.2.1 Investigate and Diagnose	assigned to a solution team that needs to provide a solution to the failure. The possible assignments are explained below: Whenever the solution team involved has a known solution, this one is sent to the SD. Afterwards "IM 2.2 Apply solution" is invoked. In all other cases a new solution is provided in which case "IM 2.3 Restore service and document solution" is invoked. The solution diagnoses activities can be influenced by the Incident Monitoring procedures, described in IM 3.1.
IM.2.2 Apply solution	**IM.2.2 Apply solution** In case of a known solution (typically a user management incident or publication), the SD applies the solution straight away. The SD closes the assignment action and invokes IM3.1.
IM.2.3 Restore service and document solution	**IM.2.3 Restore service and document solution** When the assignee of an incident (the SD, an ITSM team or an external party) provides the solution of the incident (this can imply that the service is already restored or that the solution provided allows the issuer of the incident to solve the issue himself/herself), the SD closes the assignment action and sends the solution to the issuer of the incident. Depending on the solution team involved in the resolution of the incident, they maintain their own known error list and work around lists. On this local basis these lists are updated. Incidents that have been identified as bugs (and for which a defect number is given or incidents in Known Error Lists (KEL)) are set to "Wait *for SOL"*, as the ITSM SD can only await for the final solution; the same happens in case the solution of an incident has been announced as to be delivered with the next patch or release of an application. The Incident Monitoring process (IM. 4 Incident Management – Monitoring) insures that those incidents remain followed up. The three possible outcomes of this elementary process are: • If the service has not been restored, due to the wrong assignment of the ITSM Resolver by the SD, the SD performs a functional reassignment of the incident to a more appropriate resolver; • If the service has been restored, the incident can enter the closure process IM.3; • If the service restoration is impossible (i.e. cannot be restored in the foreseen timeframe and thus to be fixed in a next release or via hotfix), then a hierarchical escalation is performed. The SD launches the escalation procedure, while the ITSM Problem Manager updates the KEL.

	IM.3 Incident Closure
IM.3.1 Communicate service restoration to Issuer	**IM.3.1 Communicate service restoration to Issuer** When a solution is provided, the SD closes the assignment action and sends the solution to the issuer of the incident with the TAXUD Thread Functional Mailbox in copy. In this e-mail the SD also asks the SDU to confirm that he/she is satisfied with the solution in order to close the incident.
IM.3.2 Check service restore	**IM.3.2 Check service restore** The issuer of the incident confirms that an acceptable solution has been provided by the SD. He/she receives an e-mail with the detail of the solution. He/she has then to reply to the SD and confirm that the service has been restored. If this is not the case, he/she also informs the SD and the incident is further processed in IM 2.1. If there is no response from the issuer after an acceptable solution is provided, the reminder on closure procedure begins and the incident is subsequently closed (IM4.2).
IM.3.3 Close incident	**IM.3.3 Close incident** An incident currently *in* status "*Wait for Info/Assigned Internal"* may be set to status "*Closed*" after the SD team has received confirmation from the requester that the solution provided was satisfactory or that all the information needed has been provided. If the incident has been opened on the initiative of the SD, the SD may proceed with closure of the incident providing adequate information in the "Suggested Solution" field of the incident actions that justify closure.
	IM.4 Incident Monitoring
IM.4.1 Check incident status	**IM.4.1 Check incident status** Occasionally replies from other parties to actions and requests from the SD may experience delays. The delayed responses to actions from 3rd parties are set to one of the following two statuses *"Assigned External"*" and "*Wait for Info"*". In all these cases the SD creates a new action and sends a reminder. The new action is assigned to the SD and its status is "*Closed"*'. The SD distinguishes between two kinds of reminders: Action reminders and Closure notifications.
IM.4.2 Issue Closure Reminder	**IM.4.2 Issue Closure Reminder** **Closure notification** For Incidents that are set to status "Wait for Info/Assigned Internal" and after the SD has already requested the closure, the

	SD sends a notification for closure reminder after 10 w-days to the user. If the user still does not reply, the SD sends a second reminder after another 10 w-days. In this reminder, the SD informs the user that his/her incident will be closed in 48 hours if the user does not reply. After this reminder, the SD can proceed with the closure of the incident after the next 48 hours unless the relevant DG TAXUD Business Thread or the user asks otherwise.
IM.4.3 Check number of previous reminders	**IM.4.3 Check number of previous reminders** The reminders sent are logged in the incident as a task, which allow the counting of reminders sent.
IM.4.4 Issue Action Reminder	**IM.4.4 Issue Action Reminder** **Action reminder** For incidents that are set to status "*Wait for Info"* or *"Assigned External*", the SD sends follow-up reminders Wait for Info on the priority level of the incident. The follow-up is performed in the following way: • Critical (Priority-1): once every w-day; • High (Priority-2): every second w-day; • Medium (Priority-3): every 5 w-days; • Low. (Priority-4): every 10 w-days. • Actions assigned to DG TAXUD C1: monthly (irrespective of the priority) Reminders are not sent when the assignee has explicitly asked reminders not to be sent before a specific due date (e.g. when a decision is planned to be discussed in a meeting). In these cases reminders are sent 1 day after the due date has passed if no reply has been received by the SD. If no answer is received following the first reminder after the due date has passed, these incidents are followed up according to the normal rule. Nevertheless, if the user has communicated to the SD that no due date has been finally planned, then the SD makes the follow-up of these incidents once a month. In case the assignee of an action has sent an e-mail notification to the SD that he/she is going to be absent for a time period and no other user is in cc of his/her request, reminders are not sent until the user has returned. Out-of-office notifications that are received from such requests may be disregarded, if they belong to specific persons, but if the request has been addressed to a central mailbox and includes more than one recipient for action the SD continues to send reminders. It is assumed in this case

	that someone else replies to the reminder. Incidents that are set to status "Assigned Internal", and for which the assignee is another ITSM party (other than the SD), are followed up closely by the SD according to their priority level if no feedback is received after the assignment. Incidents that are assigned to ITSM AM, ITSM Infrastructure, ITSM Business Monitoring are followed up every day. Incidents that concern Qualifications or Testing of full releases and which are assigned to ITSM Testing are followed up daily by the ITSM SD if no feedback received. Incidents in status *"Wait for Sol"* for which a due date has been given by an entity external to ITSM teams are followed up 1 day after the due date has passed and, if no answer is received, then reminders are sent with the frequency corresponding to low priority. If no due date is provided by the external to ITSM, incidents in status *"Wait for Sol"* are followed up once a month until a due date is specified or the deliverable is sent.
IM.4.5 Launch appropriate Escalation procedure	**IM.4.5 Launch appropriate Escalation procedure** **Action Reminders Escalation procedure (for externally assigned actions):** The 3rd action reminder to external parties is always sent CC to DG TAXUD A4/ISD, and the DG TAXUD Business Thread's Functional Mailbox asking the requester to provide the necessary information; in case no answer is given after 5 reminders, the incident is escalated to the Business Thread via an email to their Functional Mailbox. **Escalation procedure for closely followed up incidents (assigned to ITSM parties)** All incidents in the status *"Assigned Internal"* need to be closely followed up. In case incidents in the status 'Assigned Internal' have exceeded three days of inactivity, then the SD escalates these incidents to the management of the respective unit. The parties to be informed inside ITSM are: • 1st reminder – ITSM Unit, • 2nd reminder – ITSM Unit, • 3rd and final reminder – ITSM Unit ,ITSM Team Leader, ITSM Unit Manager, Incidents of Critical priority assigned to ITSM teams are

	escalated immediately to the concerned managers if no solution has been provided within the day.
IM.4.6 Implement the escalation decision	**IM.4.6 Implement the escalation decision** The issuer of the call may escalate an incident to a higher or lower priority at his/her discretion. The SD will then add an action, called the priority escalation action, to this incident, and change its priority to the requested level. This new action will be assigned to DG TAXUD A4/ISD for approval. If DG TAXUD A4/ISD approves the escalation, then the incident is set to the new escalated level. If DG TAXUD A4/ISD, rejects the escalation then the incident remains at the initial priority. The requester is notified accordingly in both cases. All critical incidents are immediately communicated by the Service Desk team via the DG TAXUD Business Sector Functional Mailbox which is kept in copy of all email exchange on these calls (except the acknowledgement email). On the other hand when an internal ITSM major priority incident occurs, then this incident is escalated inside ITSM to the list of persons below: 1. ITSM SD Manager 2. Service Support Manager; 3. Programme Director; When a user (i.e. the issuer) requests an incident to be registered on a priority level other than the one stated in the internal procedure of the SD, the SD first registers the incident according to the priority determined by the SD procedure, sends the ACK e-mail (2) template advising the issuer of the priority and asks them to provide justification if they do not agree. If the user does not respond, then no additional action is created. If the user replies with justification, a new action is opened called “Priority Escalation Request” and the SD sends an e-mail to DG TAXUD A4/ISD, for approval with the issuers e-mail attached and pastes this into the Description Field. The action is assigned and set to “Wait for Info” status. (“Wait for Info”). Once DG TAXUD A4/ISD, replies, the e-mail is forwarded to the issuer advising of the decision, the e-mail(s) is/are pasted into Solution Field and the action is set to Closed. If the incident does require change in priority, then all actions are reset to the new priority.