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

TAXATION AND CUSTOMS UNION DG
ITSM

SUBJECT:

FQP - Annex 21: Security 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	01-1	30/09/2009	Security Management split into a separate document (Annex 21), activities SEC.5 and SEC.6 added and document sent for internal review	I/R	As req.
1	01-2	16/10/2009	Implementation of internal QA comments	I/R	As req.
1	01-3	12/11/2009	Addition of CIRCA and CCN reviews	I/R	As req.
1	01-4	10/12/2009	Implementation of internal QA comments. Delivered for information to DG TAXUD	I/R	As req.

1	01-5	18/01/2010	Implementation of DG TAXUD comments. Merging of the previous SEC.1 to SEC.4 into the new SEC.1 and SEC.2.	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

DOCUMENT HISTORY 2

TABLE OF CONTENTS 4

LIST OF TABLES 5

1. INTRODUCTION 6

2. REFERENCE AND APPLICABLE DOCUMENTS 7
   - 2.1 REFERENCE DOCUMENTS 7
   - 2.2 APPLICABLE DOCUMENTS 7

3. TERMINOLOGY 8
   - 3.1 ABBREVIATIONS AND ACRONYMS 8
   - 3.2 INTERFACE WITH DG TAXUD 8

4. ITSM PROCESS MODEL 9
   - 4.1 LEVEL 0: PROCESS FLOWS 9
   - 4.2 LEVEL 1: SECURITY MANAGEMENT 10
   - 4.3 LEVEL 2: SECURITY MANAGEMENT 11
   - 4.4 LEVEL 3: SECURITY MANAGEMENT 24

List of Tables

Table 1 – Reference documents 7
Table 2 – Applicable documents 7
Table 3 – Resources subject to bi-annual reviews 15
Table 4 – RACI table 22
Table 5 – SEC Communication interfaces with DG TAXUD 23

List of Figures

Figure 4-1: ITSM Process Model 9
Figure 4-2: ITSM Process Model 10
Figure 4-3: SEC.1 Security Governance Set-up 11
Figure 4-4: SEC.2 Security Governance 12
Figure 4-5: SEC.3 Awareness 13
Figure 4-6: SEC.4 Security Incident Management 14
Figure 4-7: SEC.5a Webportal Bi-annual Reviews 16
Figure 4-8: SEC.5b Internal XXX users Bi-annual Review 17
Figure 4-9: SEC.5c CCN Bi-annual Review 18
Figure 4-10: SEC.5d CIRCA Bi-annual Reviews 19
Figure 4-11: SEC.6 User List Management 20
Figure 4-12: ITSM Security Governance Model 24
Figure 4-13: ITSMTAXUD mailbox selection 41
Figure 4-14: Collect ITSMTAXUD mailboxes 41
Figure 4-15: ITSMTAXUD mailbox selection 48
Figure 4-16: Collect ITSMTAXUD mailboxes 49

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 TAXUD) [A1], Work Package WP.0.1.

This document presents the Level 1, 2 and 3 of the ITSM process FQP - Annex 21: Security 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
R3	ISO/IEC 17799:2005	Information technology — Security techniques — Code of practice for information security management	15/06/2005	Second edition

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 General 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

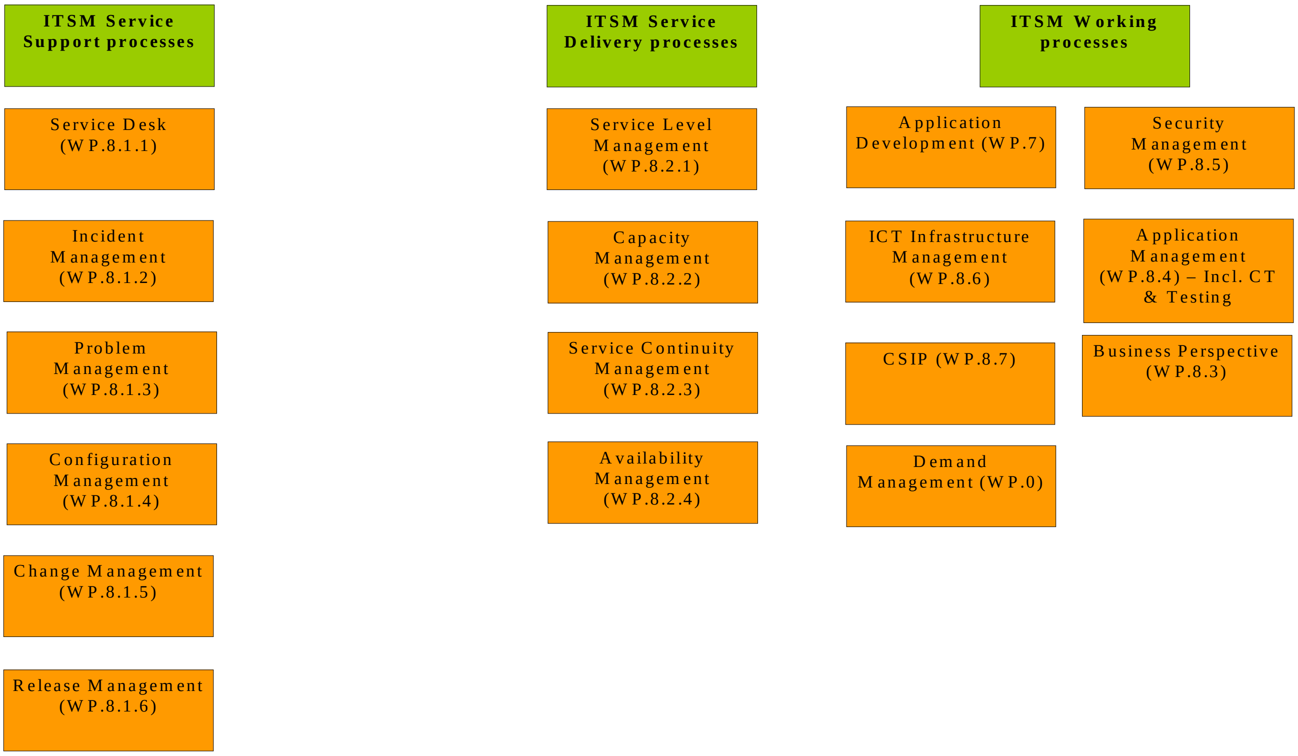

ITSM Service Support processes
Service Desk (WP.8.1.1)
Incident Management (WP.8.1.2)
Problem Management (WP.8.1.3)
Configuration Management (WP.8.1.4)
Change Management (WP.8.1.5)
Release Management (WP.8.1.6)
ITSM Service Delivery processes
Service Level Management (WP.8.2.1)
Capacity Management (WP.8.2.2)
Service Continuity Management (WP.8.2.3)
Availability Management (WP.8.2.4)
ITSM Working processes
Application Development (WP.7)
ICT Infrastructure Management (WP.8.6)
CSIP (WP.8.7)
Demand Management (WP.0)
Security Management (WP.8.5)
Application Management (WP.8.4) – Incl. CT & Testing
Business Perspective (WP.8.3)

Figure 4-1: ITSM Process Model

4.2 Level 1: Security Management

The Security Management process describes the structured fitting of security in the management organisation.

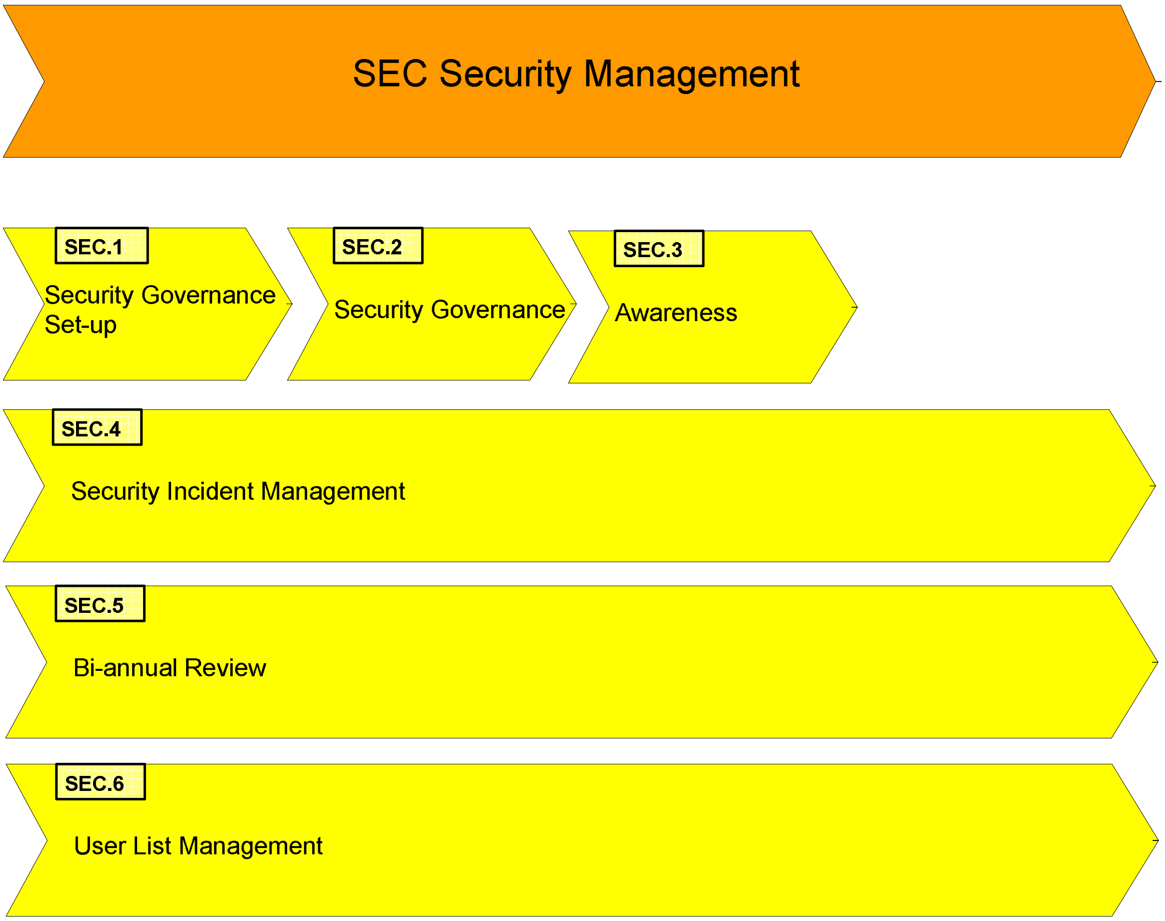


Figure 4-2: ITSM Process Model

4.3 Level 2: Security Management

SEC.1 Security Governance Set-up

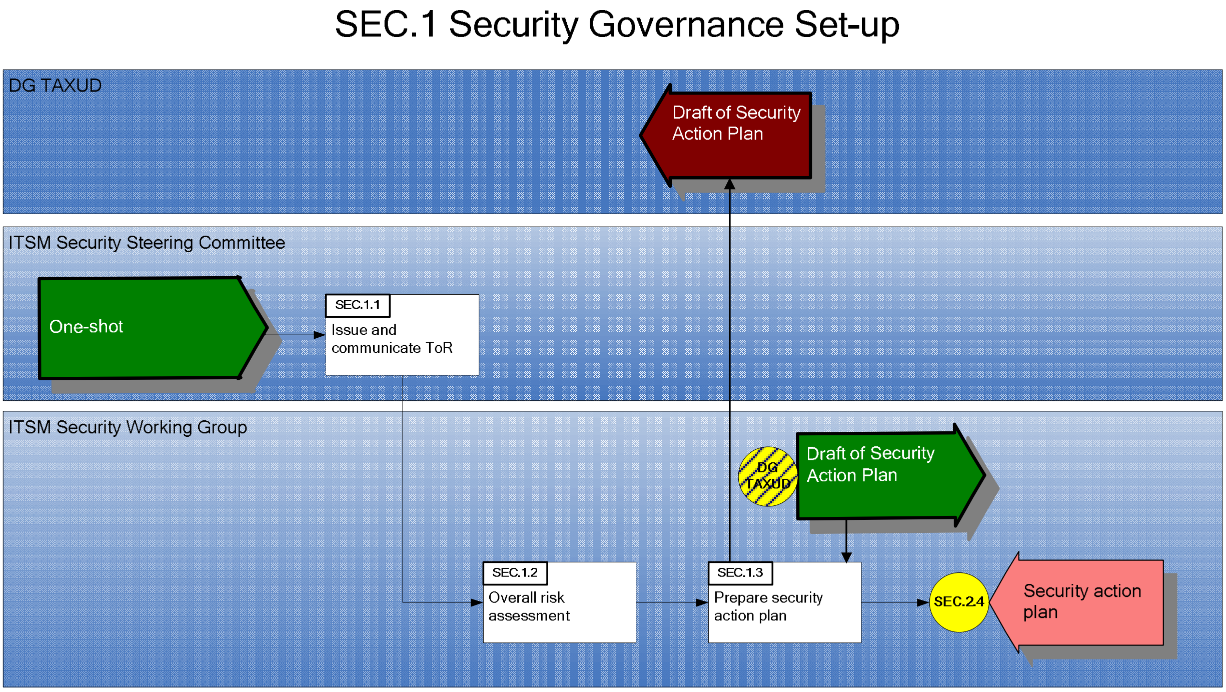

SEC.1 Security Governance Set-up
DG TAXUD
Draft of Security Action Plan
ITSM Security Steering Committee
One-shot
SEC.1.1
Issue and communicate ToR
ITSM Security Working Group
DG TAXUD
Draft of Security Action Plan
SEC.1.2
Overall risk assessment
SEC.1.3
Prepare security action plan
SEC.2.4
Security action plan

Figure 4-3: SEC.1 Security Governance Set-up

SEC.2 Security Governance

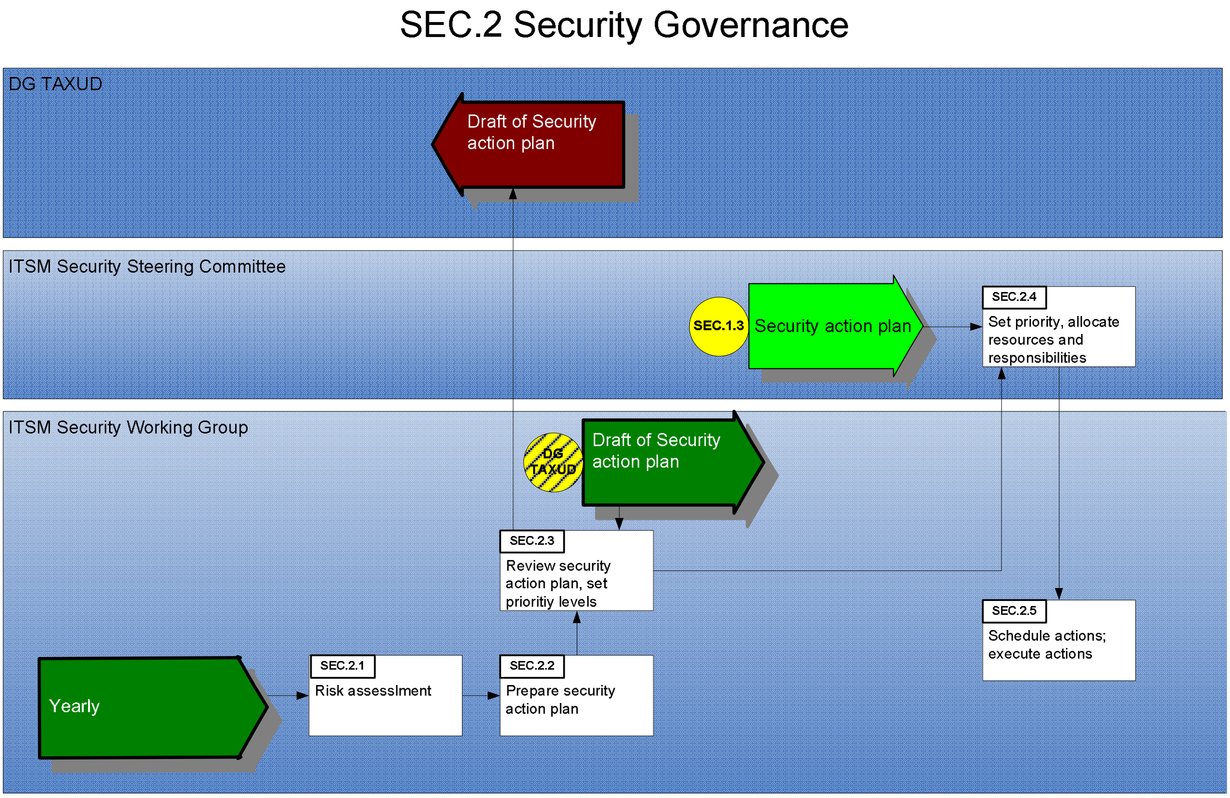
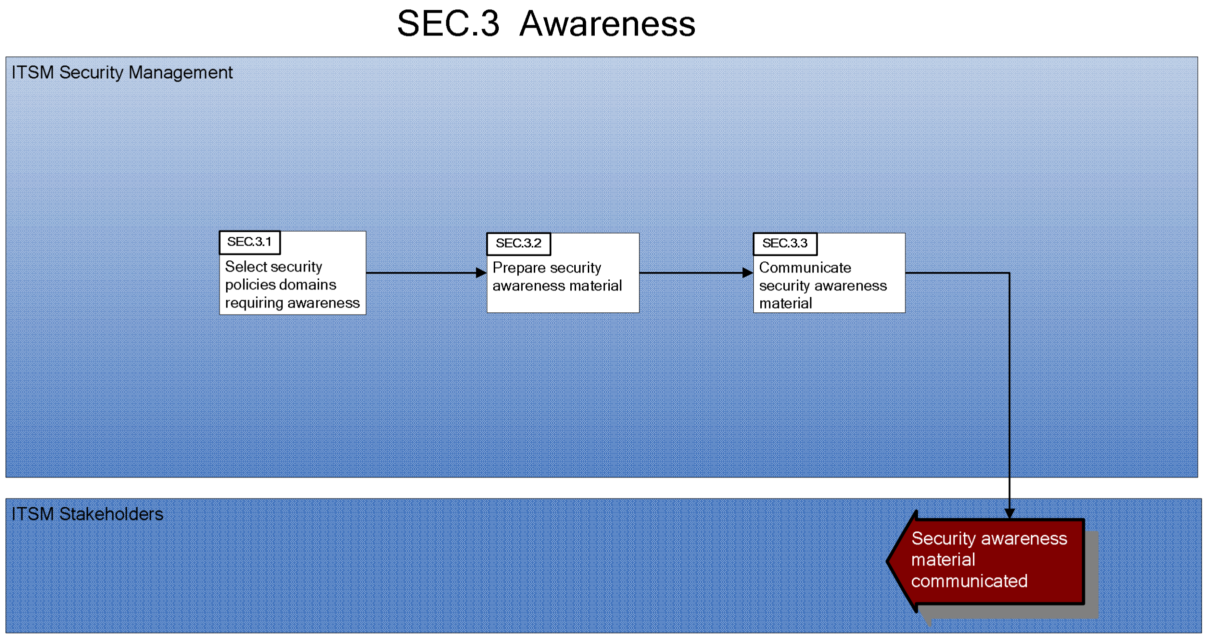

SEC.2 Security Governance
DG TAXUD
Draft of Security action plan
ITSM Security Steering Committee
SEC.1.3
Security action plan
SEC.2.4
Set priority, allocate resources and responsibilities
ITSM Security Working Group
DG TAXUD
Draft of Security action plan
SEC.2.3
Review security action plan, set prioritiy levels
SEC.2.5
Schedule actions; execute actions
Yearly
SEC.2.1
Risk assesslment
SEC.2.2
Prepare security action plan

Figure 4-4: SEC.2 Security Governance

SEC.3 Awareness



SEC.3 Awareness
ITSM Security Management
SEC.3.1
Select security policies domains requiring awareness
SEC.3.2
Prepare security awareness material
SEC.3.3
Communicate security awareness material
ITSM Stakeholders
Security awareness material communicated

Figure 4-5: SEC.3 Awareness

SEC.4 Security Incident Management

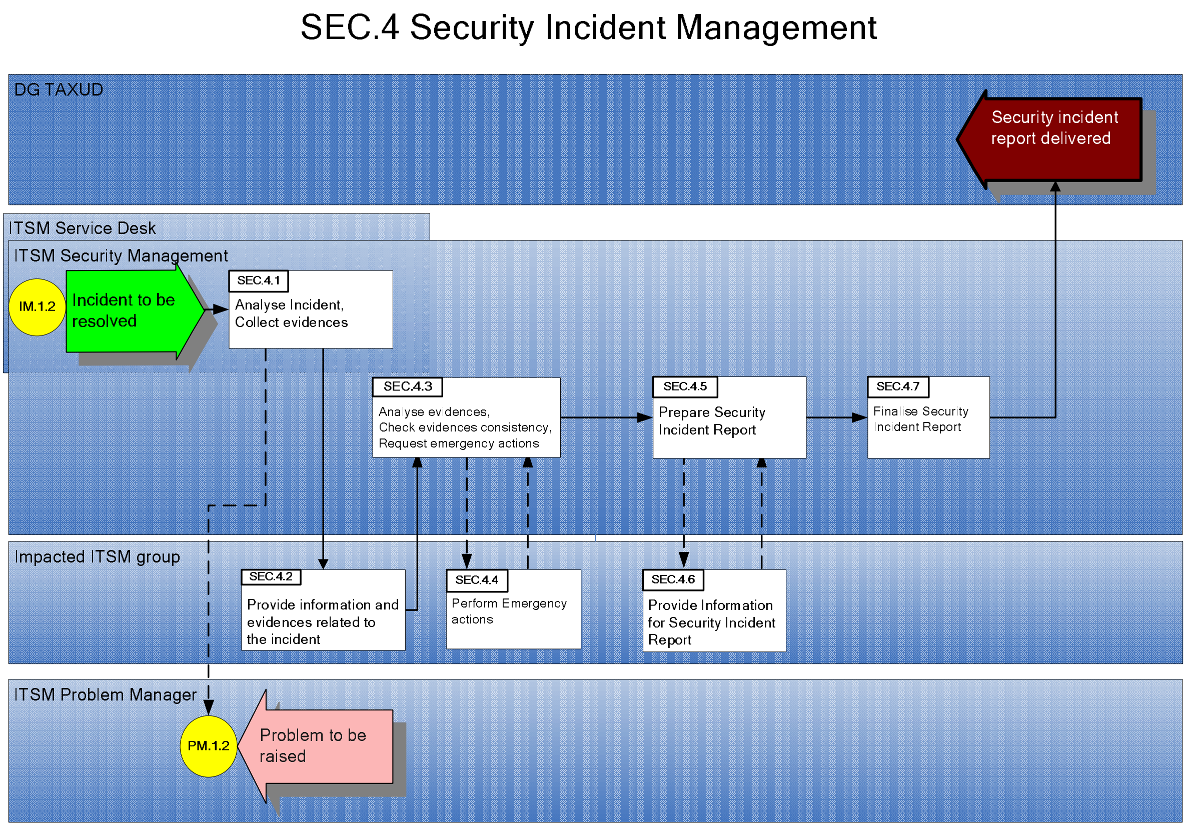

SEC.4 Security Incident Management
DG TAXUD
Security incident report delivered
ITSM Service Desk
ITSM Security Management
IM.1.2
Incident to be resolved
SEC.4.1
Analyse Incident, Collect evidences
SEC.4.3
Analyse evidences, Check evidences consistency, Request emergency actions
SEC.4.5
Prepare Security Incident Report
SEC.4.7
Finalise Security Incident Report
Impacted ITSM group
SEC.4.2
Provide information and evidences related to the incident
SEC.4.4
Perform Emergency actions
SEC.4.6
Provide Information for Security Incident Report
ITSM Problem Manager
PM.1.2
Problem to be raised

Figure 4-6: SEC.4 Security Incident Management

Remarks:

- ITSM Security Management is involved, as stated in the Security Plan (ITS-IPLN-SEC-001 §10.4), “The ITSM Security Managers coordinate the security incident management”;
- The involved incidents are those that are flagged as “security incident Yes” in ITSM SMT tool by the Service Desk.

SEC.5 Bi-annual Reviews

Table 3 below lists the resources that are subject to bi-annual review. For each resource, the provider of user list (i.e., those who can provide the list of subscribers to a resource), and the “authoritative source” (i.e., those who are competent to decide which access rights shall be kept or revoked) are provided:

Resource	**Provider of user list**	**Authoritative source**
Webportal	ITSM Service Desk	NPM’s
CCN	CCN/TC	NPM’s
CIRCA interest groups	Not applicable: no user list is provided to ITSM	IGL’s
Internal XXX resources: owITSM, ITSM collaborative tool	ITSM Infrastructure Management	ITSM Security Management with the help of other ITSM teams

Table 3 – Resources subject to bi-annual reviews

SEC.5a Webportal Bi-annual Reviews

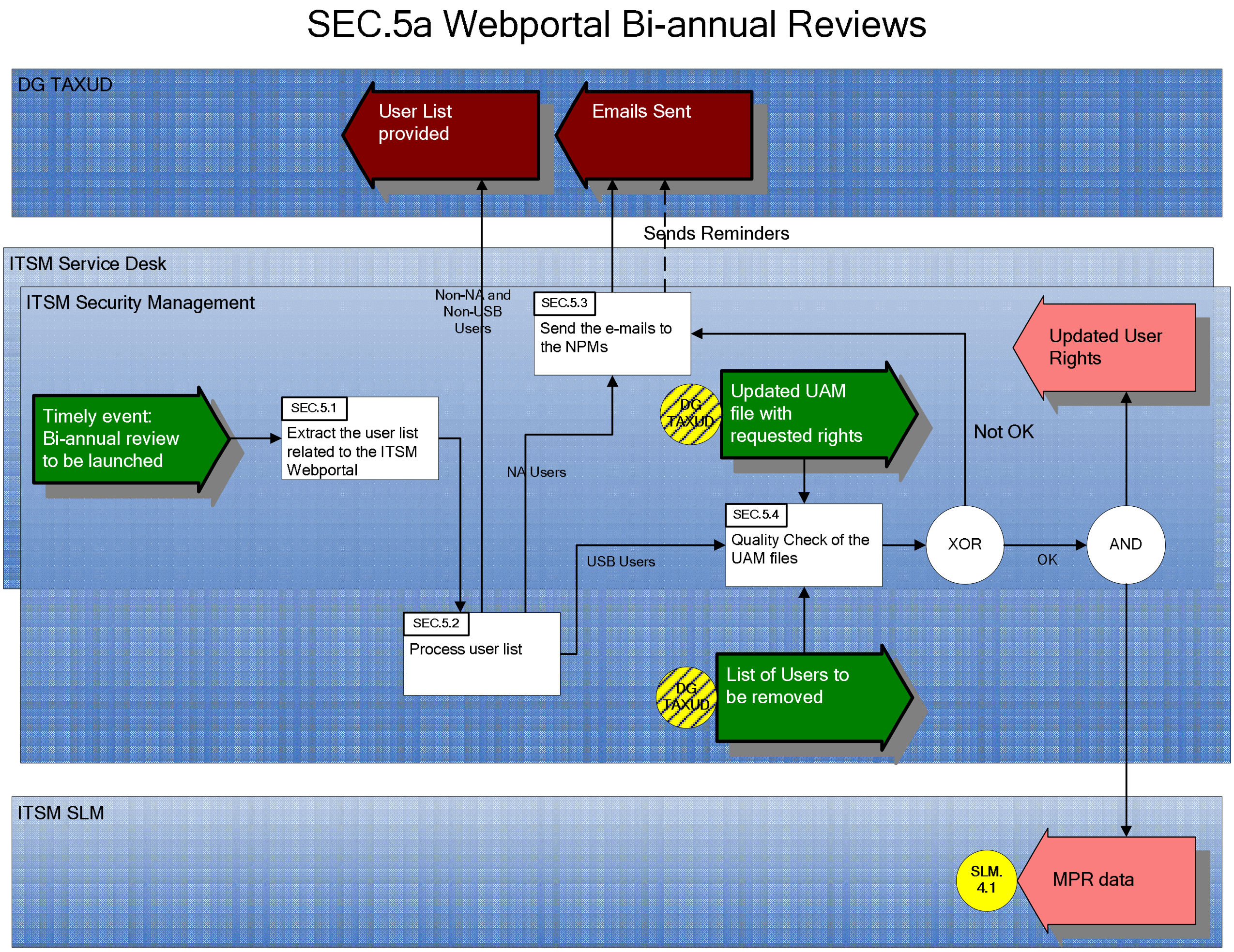

SEC.5a Webportal Bi-annual Reviews
DG TAXUD
User List provided
Emails Sent
Sends Reminders
ITSM Service Desk
ITSM Security Management
Non-NA and Non-USB Users
SEC.5.3
Send the e-mails to the NPMs
Updated User Rights
Timely event: Bi-annual review to be launched
SEC.5.1
Extract the user list related to the ITSM Webportal
DG TAXUD
Updated UAM file with requested rights
Not OK
NA Users
SEC.5.4
Quality Check of the UAM files
XOR
OK
AND
USB Users
SEC.5.2
Process user list
DG TAXUD
List of Users to be removed
ITSM SLM
SLM. 4.1
MPR data

Figure 4-7: SEC.5a Webportal Bi-annual Reviews

SEC.5b Internal XXX users Bi-annual Review

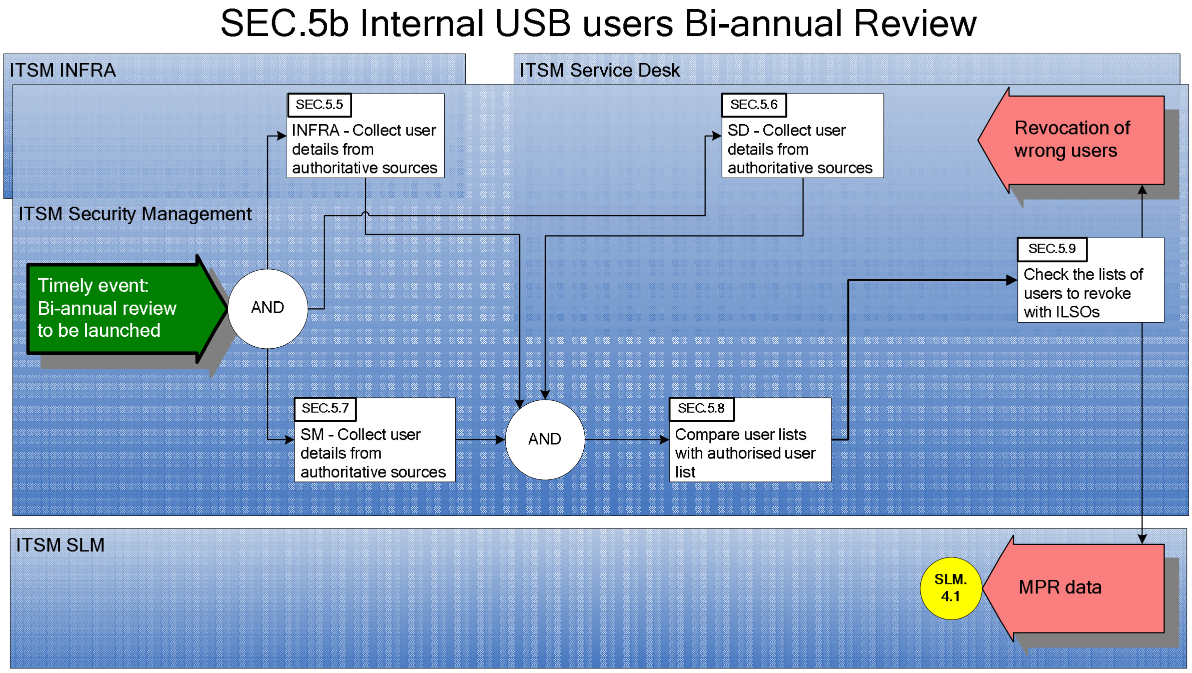
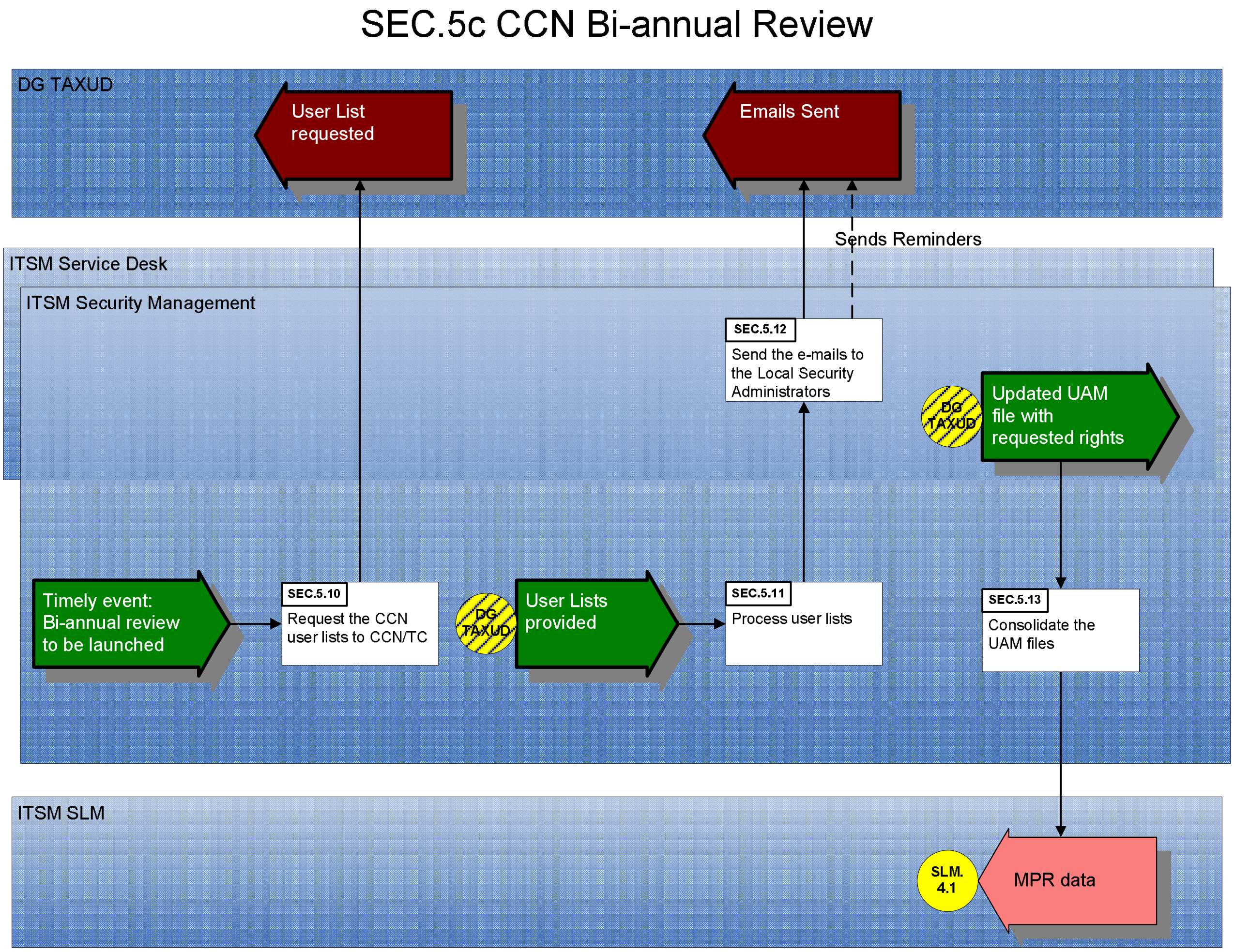

SEC.5b Internal USB users Bi-annual Review
ITSM INFRA
ITSM Service Desk
ITSM Security Management
ITSM SLM
Timely event:
Bi-annual review
to be launched
AND
SEC.5.5
INFRA - Collect user details from authoritative sources
SEC.5.6
SD - Collect user details from authoritative sources
Revocation of wrong users
SEC.5.9
Check the lists of users to revoke with ILSOs
SEC.5.7
SM - Collect user details from authoritative sources
AND
SEC.5.8
Compare user lists with authorised user list
SLM.
4.1
MPR data

Figure 4-8: SEC.5b Internal XXX users Bi-annual Review

The Internal XXX users Bi-annual Review consists of the review of the users of ITSM Collaborative Tool (ITSM presently uses KT as their Collaborative Tool; the rest of this document only uses “ITSM Collaborative Tool”), ITSM VPN, ITSM SMT and itsmtaxud mailboxes.

SEC.5c CCN Bi-annual Review



SEC.5c CCN Bi-annual Review
DG TAXUD
User List requested
Emails Sent
Sends Reminders
ITSM Service Desk
ITSM Security Management
SEC.5.12
Send the e-mails to the Local Security Administrators
DG TAXUD
Updated UAM file with requested rights
Timely event: Bi-annual review to be launched
SEC.5.10
Request the CCN user lists to CCN/TC
DG TAXUD
User Lists provided
SEC.5.11
Process user lists
SEC.5.13
Consolidate the UAM files
ITSM SLM
SLM. 4.1
MPR data

Figure 4-9: SEC.5c CCN Bi-annual Review

Remark:

With the exception of the user lists that are reviewed in process 5a, 5b and 5d, it is the CCN accounts that are used to connect to the DG TAXUD applications.

SEC.5d CIRCA Bi-annual Reviews

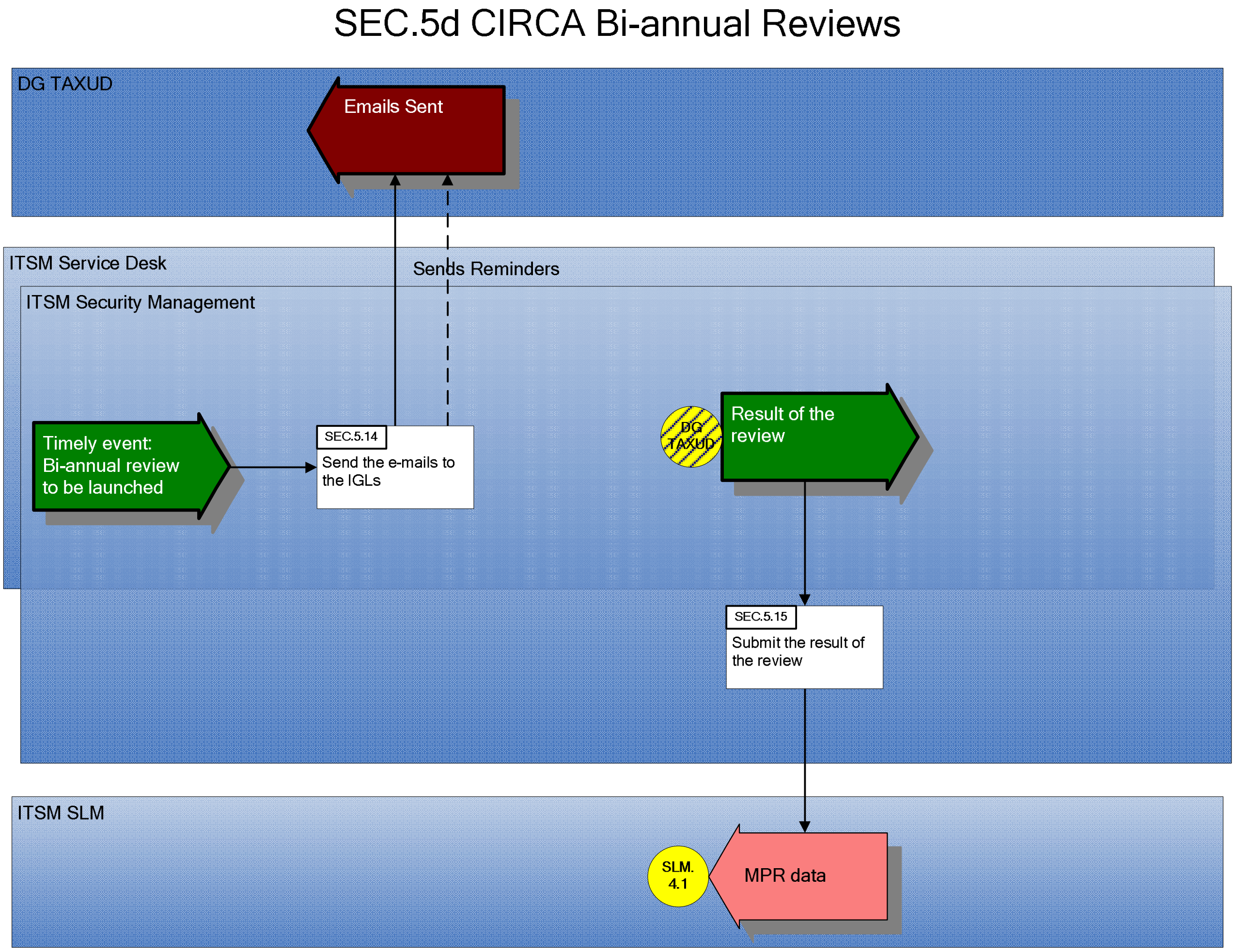


Figure 4-10: SEC.5d CIRCA Bi-annual Reviews

SEC.6 User List Management

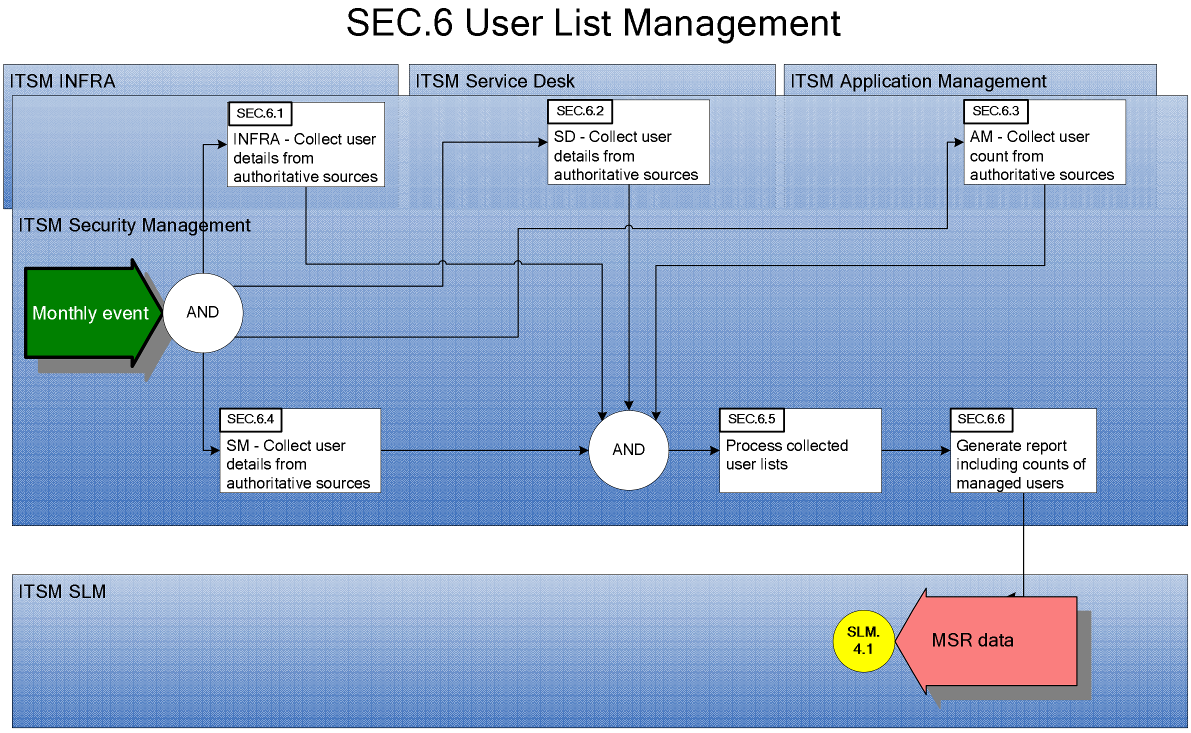

SEC.6 User List Management
ITSM INFRA
ITSM Service Desk
ITSM Application Management
SEC.6.1
INFRA - Collect user details from authoritative sources
SEC.6.2
SD - Collect user details from authoritative sources
SEC.6.3
AM - Collect user count from authoritative sources
ITSM Security Management
Monthly event
AND
SEC.6.4
SM - Collect user details from authoritative sources
AND
SEC.6.5
Process collected user lists
SEC.6.6
Generate report including counts of managed users
ITSM SLM
SLM. 4.1
MSR data

Figure 4-11: SEC.6 User List Management

Remarks:

The process starts every month on the first w-day of the month; it is based on the situation at the end of the previous month.

RACI Table for SEC

	Activity	DG TAXUD A3/LISO	DG TAXUD A3/CUST Operation Management Expert	ITSM Project Direction	ITSM Security Manager	ITSM ILSO	ITSM Application Manager	ITSM Testing	ITSM Deployment Manager	ITSM Problem Manager	ITSM Service Desk	ITSM Service Level Manager	ITSM Infrastructure Manager
SEC.1.1	Issue and communicate ToR			A/R	I	I	I	I	I		I		I
SEC.1.2	Overall Risk Assessment	C		I	A	R	R	R	R		R		R
SEC.1.3	Prepare Security Action Plan	C		I	A	R	R	R	R		R		R
SEC.2.1	Risk assessment	C		I	A	R	R	R	R		R		R
SEC.2.2	Prepare Security Action Plan	C		I	A	R	R	R	R		R		R
SEC.2.3	Review Security Action Plan; Set Priority Levels	C		I	A	I	I	I	I		I		I
SEC.2.4	Set Priority; Allocate Resources and Responsibility			A/R	C								
SEC.2.5	Schedule actions; execute actions	I		I	A	I	I	I	I		I		I
SEC.3.1	Select security policies domains requiring awareness	C		I	A	R	R	R	R		R		R
SEC.3.2	Prepare security awareness material				A/R	R	R	R	R		R		R
SEC.3.3	Communicate security awareness material	I		I	A/R	I	I	I	I	I	I	I	I
SEC.4.1	Analyse Incident Report, Collect Evidences				A	R							
SEC.4.2	Provide Information and Evidences Related to the Incident				A	R							
SEC.4.3	Analyse Evidences, Check Evidences Consistency, Request Emergency actions				A	R							
SEC.4.4	Perform Emergency actions				A	R	R	R	R		R		R

SEC.4.5	Prepare Security Incident Report				A/R								
SEC.4.6	Provide Information for Security Incident Report				A	R	R	R	R		R		R
SEC.4.7	Finalise Security Incident Report	I		I	A/R					I			
SEC.5.1	Extract the user list related to the ITSM Webportal				A						R		
SEC.5.2	Process user list				A/R								
SEC.5.3	Send the e-mails to the NPMs				A						R		
SEC.5.4	Quality Check of the UAM files		I		A/R							I	
SEC.5.5	INFRA - Collect user details from authoritative sources				A								R
SEC.5.6	SD - Collect user details from authoritative sources				A						R		
SEC.5.7	SM - Collect user details from authoritative sources				A/R								
SEC.5.8	Compare user lists with authorised user list				A/R								
SEC.5.9	Check the lists of users to revoke with ILSOs				A	R						I	
SEC.5.10	Request the CCN user lists to CCN/TC				A/R								
SEC.5.11	Process user lists				A/R								
SEC.5.12	Send the e-mails to the Local Security Administrators				A						R		
SEC.5.13	Consolidate the UAM files				A/R							I	
SEC.5.14	Send the e-mails to the IGLs				A						R		
SEC.5.15	Submit the result of the review				A/R							I	
SEC.6.1	INFRA - Collect user details from authoritative sources				A								R
SEC.6.2	SD - Collect user details from authoritative sources				A						R		
SEC.6.3	AM - Collect user count from authoritative sources				A		R						
SEC.6.4	SM - Collect user details from authoritative sources				A/R								
SEC.6.5	Process collected user lists				A/R								
SEC.6.6	Generate report including counts of managed users				A/R							I	

Table 4 – RACI table

Remark: the contractual quantities are reported in the MPR and MSR.

Communication interfaces with DG TAXUD

Interface description communication with DG TAXUD	Direction	Format
SEC 1.3 Prepare Security Action Plan	Outgoing	Encrypted E-mail
SEC 1.3 Prepare Security Action Plan	Ingoing	Encrypted E-mail
SEC 2.2 Prepare Security Action Plan	Outgoing	Encrypted E-mail
SEC 2.2 Prepare Security Action Plan	Ingoing	Encrypted E-mail
SEC 4.7 Finalise Report	Outgoing	Paper
SEC 5.2 Process user list	Outgoing	E-mail
SEC 5.3 Send the e-mails to the NPMs	Outgoing	E-mail from SD to NPM
SEC 5.4 Quality Check of the UAM files	Ingoing	E-mail from NPM to SD
SEC 5.10 Request the CCN user lists to CCN/TC	Outgoing	E-mail to CCN TC
SEC 5.11 Process user lists	Ingoing	E-mail from CCN TC
SEC 5.12 Send the e-mails to the Local Security Administrators	Outgoing	E-mail from SD to LSA
SEC 5.13 Consolidate the UAM files	Ingoing	E-mail from LSA to SD
SEC 5.14 Send the e-mails to the IGLs	Outgoing	E-mail from SD to IGL
SEC 5.15 Submit the result of the review	Ingoing	E-mail from IGL to SD

Table 5 – SEC Communication interfaces with DG TAXUD

4.4 Level 3: Security Management

Procedure

SEC.1.1

Issue and communicate ToR

SEC.1 Security Governance Set-up

SEC.1.1 Issue and communicate ToR

This process is carried out within the Security Steering Committee. The Security Steering Committee is installed and chaired by the ITSM Project Director.

Governance Model – The ITSM Governance has two levels: Security Steering Committee, and Security Working Group, see Figure 4-12 below:

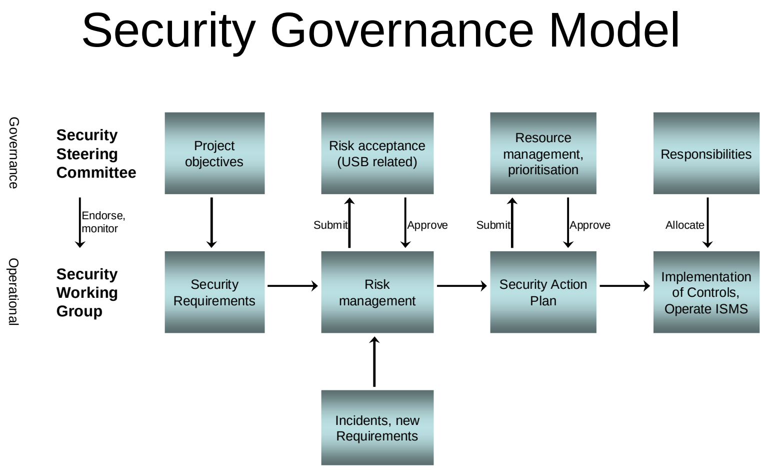

Security Governance Model
Governance
Security Steering Committee
Project objectives
Risk acceptance (USB related)
Resource management, prioritisation
Responsibilities
Endorse, monitor
Submit
Approve
Submit
Approve
Allocate
Operational
Security Working Group
Security Requirements
Risk management
Security Action Plan
Implementation of Controls, Operate ISMS
Incidents, new Requirements

Figure 4-12: ITSM Security Governance Model

The responsibilities of the Security Steering Committee are merged into the XXX Project Committee, which has at least one representative of each XXX Consortium company in the Committee.

The responsibilities of the Security Steering Committee are:

1. Monitor/review actions by the Security Working Group (see below the tasks of the Security Working Group);

2. Express project objectives;
3. Accept residual risks as far as these residual risks are related to the IT management carried out by the XXX Consortium for DG TAXUD;
4. Set priorities for actions that are proposed by the Security Working Group;
5. Allocate resources for security-related actions; allocate responsibilities for implementation;
6. Approve internal security policies before their inclusion into the ISMS.

The tasks of the Security Working Group are:

1. Identify security requirements; identify new needs for security (e.g., new requirements from DG TAXUD or audit recommendations); identify and evaluate related risks;
2. Analyse security incidents; identify and evaluate risks;
3. Identify residual risk that is related to the IT management carried out by the XXX Consortium; submit this residual risk for acceptance by Security Steering Committee;
4. Develop a plan to cover new needs and to mitigate identified risks; submit the plan to the Security Steering Committee for approval, prioritisation and resource allocation;
5. Schedule security-related actions according to priorities and resources allocated by the Security Steering Committee; implement controls;
6. Monitor the progress of security-related actions:
    - The ITSM Security Manager performs the monitoring on a day-by-day basis;
    - The Security Working Group performs the monitoring at the rate of his meetings.
7. Submit every change in the ISMS to the Security Steering Committee for approval;
8. Publish approved policies and procedures; communicate them to all XXX team members;
9. Report:

- To the Security Steering Committee about their activities and the issues they encounter;
- To DG TAXUD A3/LISO and to the Security Steering Committee about the composition of the Security Working Group;
- To DG TAXUD A3/LISO about their activities (ITSM Security Manager is the contact point for DG TAXUD A3/LISO). If DG TAXUD A3/LISO does not agree with the schedule of security-related activities, he escalates the issue to the Security Steering Committee (escalation path is to be decided with DG TAXUD A3/LISO);
- Note: the monthly reporting (annexed to the MPR) is performed by the ITSM Security Manager.

The Security Working Group is chaired by the ITSM Security Manager; the other members of the Security Working Group are ILSO's (Information Local Security Officers). Each ITSM team that is concerned with security shall have a representative in the Security Working Group (security concerned teams: Infrastructure Management, Application Management, testing team, Service Desk, Problem Management, and deployment office). The ILSO responsibilities are of two kinds:

1. Responsibilities within the Security Working Group: the ILSO's cooperate with the ITSM Security Manager to perform the tasks described above;
2. ILSO's also have day-to-day responsibilities, which they exercise as a virtual team (i.e., via e mail communication; no meetings), among others:
    - Act as the relay of the ITSM Security Manager in his/her team, by performing or co-ordinating day-to-day security-related tasks;
    - Monitor how the security policies are implemented in his/her team; report to the ITSM Security Manager about any compliance issue;
    - Perform emergency actions that are required to fix Security Incidents and report to the ITSM Security Manager about the result;
    - Participate to the analysis of Security Incidents by collecting evidences and providing them to the ITSM Security Manager.

Security Governance Set-up – The Security Steering Committee issues and publishes the Terms of Reference (ToR) of the Security Working Group. The proposed contents of the ToR (to be developed by ITSM Security Management in cooperation with ITSM Project Direction) are:

- Information security requirements for the ITSM project, derived from § 3.7 of the technical annex of the ITSM invitation to tender;
- A description of the two-layer security governance model, including the responsibilities and the way of working of the Security Working Group (see above);
- A statement to all XXX team members:
    - The statement demonstrates support for, and commitment to, information security by the ITSM project direction;
    - Through this statement, the ITSM project direction declares that his support is provided through the issue and maintenance of information security policies and procedures across the team; the policies and procedures will be part of an ISMS, which is located in a ITSM Webportal real accessible to everyone;
    - The statement notifies every team member that he/she shall comply with the policies and procedures that are published in the ISMS.

The ITSM Project Direction distributes the ToR to all XXX team members. To make it understandable and directly applicable by all intended readers, the ToR shall be short and to the point (2 to 3 pages; bullet points).

SEC.1.2

Overall risk assesslment

SEC.1.2 Overall Risk Assessment

This is an initial risk management exercise based on a methodology that is drawn from ISO/IEC 27005:

Risk Assessment – The steps are:

- <u>Context establishment</u>: the context is the one of the ITSM project. The Security Working Group produces a draft, which the ITSM Security Manager submits for information to DG TAXUD A3/LISO; DG TAXUD A3/LISO input (if any) is validated by ITSM Security Management;
- <u>Risk assessment</u>: a draft of a risk assessment report is produced by the Security Working Group; it includes a list

of the target assets, and an identification of the threats (taking into account the list of IT security risks from the technical annex of the ITSM Invitation to Tender), of the existing controls, of the vulnerabilities and of the impacts. The Security Incident Reports, which have been produced since the last risk assessment, are also used to identify risks. The draft of the risk assessment report is then used as a basis for a risk assessment workshop;

- Workshop: the risk assessment workshop groups the Security Working Group and DG TAXUD A3/LISO. Based on the results of the workshop, ITSM Security Management produces a definitive version of the risk assessment report, which provides a description of the risk posture of IT under the ITSM project.

Risk estimation – It is based on the risk assessment report. It includes:

- The assessment of the impacts and the likelihood of threats: a draft is produced by the Security Working Group; this draft is then used as a basis for a risk estimation workshop;
- Workshop: the risk estimation workshop groups the Security Working Group and DG TAXUD A3/LISO. During the workshop, DG TAXUD/A3 LISO relies on his own priorities as well as on the risk posture as described in the risk assessment report in order to help setting priority levels. The deliverable of the workshop is a risk estimation report including the list of risks to treat in priority.

SEC.1.3
Prepare security action plan

SEC.1.3 Prepare security action plan

The steps are:

- The Security Working Group drafts a security action plan containing risk reduction controls to mitigate the identified risks. The Security Working Group uses reference document [R3] as a base for the selection of risk reduction controls;
- The ITSM Security Manager discusses the security action plan with DG TAXUD A3/LISO in order to come to an agreed content and a level of priority (“low”, “medium”, “and high”) for each action.

SEC.2.1
Risk assessment

SEC.2 Security Governance

SEC.2.1 Risk assessment

This is a risk management exercise that shall occur at least yearly; other events may trigger it: evolution of architecture, new risks, problem management, etc. The risk management exercise is based on a methodology that is drawn from ISO/IEC

27005. The process is identical to the process SEC.1.2.

SEC.2.2

Prepare security action plan

SEC.2.2 Prepare security action plan

This is identical to the SEC.1.3 process.

SEC.2.3

Review security action plan, set prioritiy levels

SEC.2.3 Review security action plan; set priority levels

The ITSM Security Manager discusses the security action plan with DG TAXUD A3/LISO in order to come to an agreed content and a level of priority (“low”, “medium”, “and high”) for each action.

SEC.2.4

Set priority, allocate resources and responsibilities

SEC.2.4 Set priority; allocate resources and responsibility

The Security Working Group submits the Security Action Plan to the Security Steering Committee.

The Security Steering Committee sets priorities for actions that are included in the Security Action Plan; it allocates resources for security-related actions; it allocates responsibilities for implementation.

SEC.2.5

Schedule actions; execute actions

SEC.2.5 Schedule actions; execute actions

The Security Working Group

- Schedules security-related actions according to priorities and resources allocated by the Security Steering Committee;
- Implements the controls contained in the security action plan;
- Monitors the progress of security-related actions;
- If there is a change in the ISMS, it submits it to the Security Steering Committee for approval;
- Reports:
    1. To the Security Steering Committee about their activities and the issues they encounter;
    2. To DG TAXUD A3/LISO about their activities.

SEC.3.1

Select security policies domains requiring awareness

SEC.3 Do: Awareness

SEC.3.1 Select security policies domains requiring awareness

Each year, the ITSM Security Manager reviews the change in the following areas:

- Compliance with legislative, EC regulatory and ITSM contractual requirements;
- Security education, training, and awareness requirements;
- Business Continuity Management;
- Consequences of information security policy violations;
- General and specific responsibilities for information security management, including reporting information security incidents;
- Reference to documents supporting the policies, such as standards, guidelines and procedures for specific information systems or security rules users should comply with;
- In addition to the above, the ITSM Security Manager takes into account new training requirements that may come from the annual risk assessment activity.

The ITSM Security Manager selects the changes that are sufficiently significant to require a change in the behaviour of XXX Consortium users.

If the security awareness campaign is not the first one in the ITSM project, the ITSM Security Manager assesses the success of the previous awareness campaign through the analysis of the success indicators (see SEC.3.2), and proposes ways to reach a higher success.

SEC.3.2

Prepare security awareness material

SEC.3.2 Prepare security awareness material

Every year, based on the work produced in SEC.3.1 above, the ITSM Security Manager decides on a one-year awareness communication plan, which consists of:

- The message to deliver:
    - Key communication messages (e.g., top 10 tips);
    - Which risks and threats to focus on, what is relevant to XXX Consortium users;
    - What to do and not to do.
- The transmission channels to use (newsletter, events, posters, screen savers, intranet site…); a choice between an ongoing campaign and a one-off effort;
- An estimation of the needed resources in terms of manpower;
- Indicators to measure the success of the awareness programme:
    - The amount of security incidents caused by a

member of the XXX Consortium that are recorded in a year;

    - If a security awareness event is organised: the number of invited people versus the number of attendees. The latter is based on an attendance record maintained by the ITSM Security Manager.

SEC.3.3
Communicate security awareness material

SEC.3.3 Communicate security awareness material

The ITSM Security Manager executes the communication plan as described in SEC.3.2 above, while:

- Monitoring the consumption of resources in order to be able to allocate extra resources in due time, should the consumption go beyond the estimation made in SEC.3.2;
- Monitoring the success indicators defined in SEC.3.2.

SEC.4.1
Analyse Incident, Collect evidences

SEC.4 Security Incident Management

SEC.4.1 Analyse Incident, Collect evidences

Incidents are observed by ITSM Monitoring, ITSM Application Management, ITSM Infrastructure Management, etc. who inform ITSM Service Desk. The subsequent steps are as follows:

- **Detection** – Each time the ITSM Service Desk creates or modifies an incident the ITSM SMT, ITSM Service Desk scans the description of the incident to check if it contains one or more keywords as provided in a list, which is included in the ITSM Security Incident Handling Procedure (SIHP, reference ITSM-IP-172). The scan includes the header of e-mails (including the originators' addresses) and the body of e-mails. Attachments are not scanned. The list of keywords to recognise is included in the internal procedure 171 (Security Incident Handling Procedure, ref. ITSM-IP-171). If any of the keywords in the list is present, ITSM Service Desk:
    - Flags the incident as "security";
    - Sends an e-mail to security@itsmtaxud.europa.eu with the incident reference.
- **Screening of false positives** – On receipt of the e-mail from ITSM Service Desk, a member of the ITSM Security Management team analyses the incident with the help of other ITSM teams as needed; ITSM Infrastructure Management or ITSM Application Management may be involved. If the analysis reveals that the incident is not a security incident (definition: An information security incident is an event –or a chain of events– that compromises

the confidentiality, integrity or availability of DG TAXUD’s information), The ITSM Security Manager sends an e-mail to ITSM Service Desk, asking to remove the “security” flag, and the process stops here as far as security is concerned;

- **Analysis** – ITSM Security Manager analyses the available information contained in the Incident description as recorded in the ITSM SMT. This analysis includes a study whether the security incident is a “routine incident”, i.e., an incident that can be dealt with at once by ITSM. A vast majority of security incidents that have occurred are “routine incidents”, for example:

  1. <u>Application down, or abnormally slow</u> – Generally this type of incident is dealt with by ITSM Monitoring, ITSM Infrastructure Management or ITSM Application Management: the server or the application is restarted, or a non critical activity (e.g., a report generation on a server that is also running applications) is stopped;

  2. <u>Disk free space low</u> – Generally this type of incident is dealt with by ITSM Application Management, e.g., by compacting or cleaning files;

  3. <u>Unscheduled unavailability of NA</u> – Generally this type of incident is dealt with by the NA, and the action by ITSM consists in a notification to the NA.

  If the security incident is a “routine incident”, process stops here (as far as ITSM Security Management is concerned); else the incident needs a specific reaction, and the process continues with the next step;

- **Correlation** – The ITSM Security Manager attempts to correlate the incident with other incidents that have been raised by the ITSM Service Desk and for which there is a direct relationship with the current Security Incident. If a correlation is discovered, the ITSM Security Manager looks for the related actions that have been already taken to tackle those other incidents, by whom, when and the outcome of the actions undertaken to resolve them. The ITSM Security Manager also looks for the root cause of the related incidents.

If the incident is not a “routine incident” the ITSM Security Manager proceeds to the next step.

SEC.4.2

Provide information and evidences related to the incident

SEC.4.2 Provide information and evidences related to the incident

The ILSO’s from the relevant ITSM support groups (e.g. ITSM

Infrastructure Management or ITSM Application Management) are contacted by the ITSM Security Manager in order to gather technical evidences contained in the systems and/or applications logs. In the case the information is only available from DIGIT, ITSM opens a ticket in the DIGIT SMT.

The ILSO’s of the ITSM support groups involved shall communicate in written form the necessary information back to the ITSM Security Manager.

SEC.4.3
Analyse evidences,
Check evidences consistency,
Request emergency actions

SEC.4.3 Analyse evidences, check evidences consistency, request emergency actions

With the information compiled by the relevant ILSO’s, the ITSM Security Manager performs the following actions:

- A check to ensure that all the necessary information is collected, relevant, and is sufficient to prepare the emergency actions that will be executed by the appropriate ILSO’s;
- A review of the emergency actions that have been applied at once by ITSM Service Desk, ITSM Infrastructure Management or ITSM Application Management;
- When supplementary emergency actions are required, a request for emergency actions is prepared by the ITSM Security Manager and distributed across the ITSM organisation to the appropriate ILSO’s who are responsible to perform those actions. Requests for emergency actions are detailed by system, impact and urgency.

SEC.4.4
Perform Emergency actions

SEC.4.4 Perform Emergency actions

According to the information distributed by the ITSM Security Manager, the ILSO’s perform the required actions and indicate the success or failure of the actions to ITSM Security Management, as well as the observed results of the actions in relation with the ongoing incident.

This procedure may be iterative until the expected results are obtained. Real-time communication between the ILSO’s and the ITSM Security Manager is mandatory, preferably by e-mail.

SEC.4.5
Prepare Security Incident Report

SEC.4.5 Prepare Security Incident Report

Security Incident Reports are produced only for incidents that:

- Were flagged by ITSM Service Desk (see SEC.4.1 process above),
- That are neither false positive nor routine incidents, and

- That 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”.

When such a Security Incident is under control, and normal service operation has been restored, the ITSM Security Manager starts writing the Security Incident Report.

The Security Incident Report contains:

- A brief chapter analysing the e-mail communications exchanged between ITSM team members and/or with DG TAXUD representatives and directly related to the security incident;
- When available, an analysis of the different logs files as compiled by the respective ILSO’s;
- A detailed analysis of the Security incident in itself, from detection and registration to resolution, recovery and closure;
- A gap analysis when applicable, to cross check the requirements of the Security Policy with the findings of the ITSM Security Manager as related to infrastructure components, systems and data involved;
- Recommendations and request for changes to implement in order to avoid the security incident to reoccur in the future. This can include several change requests as well.

SEC.4.6

Provide Information for Security Incident Report

SEC.4.6 Provide Information for Security Incident Report

During the writing of the Security Incident Report, the collection of additional information from the ITSM support groups is centralised by the ILSO’s upon ITSM Security Manager request. This may include, but is not limited to:

- Self assessment compared to ITSM Security Policy;
- Gap analysis;
- Recommendations.

SEC.4.7

Finalise Security Incident report

SEC.4.7 Finalise Security Incident Report

The writing of the final Security incident report is finalised by the ITSM Security Manager.

The Security Incident report is proposed for review (internal review cycle) before it is communicated to DG TAXUD

A4/PSU and DG TAXUD A3/LISO.

SEC.5 Bi-annual Review

SEC.5.1

Extract the user list related to the ITSM Webportal

SEC.5.1 Extract the user list related to the ITSM Webportal

ITSM Security Manager requests to ITSM Service Desk the user list related to the ITSM Webportal. The information is sent under the form of an excel file; it reflects the current situation as listed below:

One row per user, containing at least:

- Full name – Last name, First name;
- New UID – The ID of the user account;
- Organisation – The organisation (NA, Commission, contractor…) the user is working with;
- CS/RD Domain – CS/RD domains that are accessible by the user: NCTS, ECS, ICS and/or EO;
- CS/RD TST – Rights on CS/RD test domain: it is either empty, or it contains “Full”, “No”, “Read” or “Write”;
- CS/RD PROD – Rights on CS/RD production domain: it is either empty, or it contains “Full”, “No”, “Read” or “Write”;
- CS/MIS Domain – CS/MIS domains that are accessible by the user. The values are:

Value	Domains
E	ECS
I	ICS
N or NCTS	NCTS
EI	ECS and ICS
EN	ECS and NCTS
IN	ICS and NCTS
EIN or B	ECS, ICS and NCTS

- CS/MIS – CS/MIS profile of the user. The values are: Admin, ND Admin, ND User and Oper (for operator);
- E-mail – E-mail address of the user;
- Deleted – “FALSE” if the user is still active; “TRUE” otherwise.

SEC.5.2

Process user list

SEC.5.2 Process user list

When the list is delivered, the ITSM Security Manager processes as follows:

- Remove useless information. Only the content that is described in the step above remain (note: the user list contains information that is useless in this context, e.g., phone numbers or postal address);
- Remove disabled users;
- Remove duplicates. It is possible that two accesses have been created for the same user; generally when it is the case both accounts have the same User ID, Last name and First name (sometimes with typo differences). If the ITSM Security Manager can clearly identify the “correct” account, he removes the other one from the excel sheet, otherwise the ITSM Security Manager requires ITSM Service Desk to send an e-mail to the responsible manager for identification of the correct duplicate. When all “wrong” duplicates are identified, the ITSM Security Manager requires ITSM Service Desk to disable them;
- For each XXX team, the ITSM Security Manager makes a list of XXX users that are present in a user list but absent of the authorised user list (Annex 4 of MPR);
- The ITSM Security Manager sends each list of XXX users that are not in the authorised user list to the ILSO of the team. The ILSOs check that the users of the lists do not work anymore on ITSM and send the confirmation to ITSM Security Management;
- The ITSM Security Manager sends the list of users who were not identified by the ILSOs to the ITSM Projects directors for a final confirmation;
- For the non-NA and non-XXX users of ITSM Webportal (which contains users of the commission and other contractors) the list of users is sent to the DG TAXUD A3/LISO for checking. The LISO dispatches the user list to people able to identify the accounts that are not required anymore;
- For each NA, the ITSM Security Manager copies the information related to the NA in an excel sheet formatted for the Webportal Bi-annual review (at the moment of the delivery of the FQP, it is located on ITSM Collaborative Tool under: “Browse » Folders » ITSM Project (XXX) » 04. Security Management » Webportal user access review » TAXUD-ITSM-Portal-UAM-yyyyQq-na.xls”), updates the date reported in cell “B2” (of the Excel file), protects the

data (to prevent the NPMs from updating the wrong cells), and saves the file under the name “TAXUD-ITSM-Portal-UAM-yyyyQq-na” (where yyyy is the current year, q is the number of the quarter of the year and na is the two letter code of the NA).

SEC.5.3
Send the e-mails to the NPMs

SEC.5.3 Send the e-mails to the NPMs

- For each NA, the ITSM Security Manager prepares an e-mail by editing a copy of the e-mail formatted for the Webportal Bi-annual review (at the moment of the delivery of the FQP, it is located on ITSM Collaborative Tool under: “Browse » Folders » ITSM Project (XXX) » 04. Security Management » Webportal user access review » Bi-annual review of user accesses of. zip”). The ITSM Security Manager attaches the excel sheet to the e-mail, enters the NPMs’ e-mail addresses in the “To:” field, adds the two letter code of the NA at the end of the “Subject:” field, saves it and renames the file by adding the two letter code of the NA at the end of the name;
- The ITSM Security Manager creates a ZIP archive with all the prepared e-mails and send it to ITSM Service Desk;
- For each e-mail file, ITSM Service Desk opens the file and sends the e-mail;
- Before attaching the e-mails to the incident on ITSM SMT, ITSM Service Desk removes the excel sheets (for confidentiality reasons, as it is accessible through the ITSM Webportal);
- After two weeks, ITSM Service Desk sends a reminder to the Interest Group Leaders (who manage the CIRCA interest group member lists) that have not yet replied;
- Two weeks later, ITSM Service Desk sends a reminder to the Interest Group Leaders (who manage the CIRCA interest group member lists) that still have not yet replied.

SEC.5.4
Quality Check of the UAM files

SEC.5.4 Quality Check of the UAM files

- On receipt of an e-mail from NPMs, the ITSM Service Desk forwards any registration forms to DG TAXUD A3/CUST MS Coordination Assistant for approval and follows the normal user registration process (under a separate incident);
- The ITSM Service Desk forwards the complete answers of the NPMs to ITSM Security Management (with DG TAXUD A3/CUST Operation Management Expert in copy);
- Before attaching the e-mails to the incident on ITSM SMT,

the ITSM Service Desk removes the excel sheets (for confidentiality reasons as it is accessible through the ITSM Webportal);

- The ITSM Security Manager makes a quality check of the excel files received form the NPMs. In case of inconsistencies or if the NPMs have asked for something that is not allowed (for example if the NPMs have asked for write access in CS/RD Production for more than 3 users), the ITSM Security Manager prepares new queries for the NPMs and asks the ITSM Service Desk to send them to the NPMs;
- In the excel sheets which have passed the quality check and in the user lists from other sources (the user list received from the DG TAXUD A3/LISO and the XXX user list checked by the ILSOs and the ITSM Projects directors), the ITSM Security Manager underlines the users to disable and the changes in user rights and sends the files to the ITSM Service Desk (with DG TAXUD A3/CUST Operation Management Expert in copy for the users of NA);
- The ITSM Service Desk updates the users according to the answers sent by the ITSM Security Manager and informs the NPMs that the changes have been done.
- The ITSM Security Manager submits the result of the review to Service Level Management (WP.8.2.1) for bundling into the current month’s MPR.

SEC.5.5

INFRA - Collect user details from authoritative sources

SEC.5.5 INFRA – Collect user details from authoritative sources

This is a periodic activity that ITSM Infrastructure Management launches twice a year at ITSM Security Managers request (when the process is started at a beginning of a month the ITSM Security Managers use the data obtained in SEC.6.1). It consists in the provision of user lists to ITSM Security Management.

User lists – ITSM Infrastructure Management provides user lists related to the following ITSM IT resources:

- ITSM Collaborative Tool;
- ITSM VPN.

The information is sent under the form of an Excel file; it reflects the current situation. The authoritative sources related to each IT resource are listed below:

IT resource	**Source**
ITSM Collaborative Tool	The user list of the application.
VPN	An Excel workbook, which is maintained by ITSM Infrastructure Management on a daily basis.

ITSM Infrastructure Management extracts the user details from these sources, and exports the user details to Excel workbooks when the source is not itself an Excel workbook.

The content is:

IT resource	**Contents**
ITSM Collaborative Tool	One row per user, containing at least: • Full name – Last name, First name; Userid – The first 4 characters of a userid are “XXX.” (For XXX team members), “txd.” (For DG TAXUD), or “lot.” (For non-ITSM contractors). Userids that start neither with “XXX.”, “txd.”, nor with “lot.” refer to support users (e.g., the ITSM Collaborative Tool administrator) or to disabled ones.
VPN	One row per user, containing at least: • Full name – Last name, first name; Active Y/N – Contents is “Y” for active VPN connexions; it is “N” for inactive ones.

SEC.5.6

SD - Collect user details from authoritative sources

SEC.5.6 SD – Collect user details from authoritative sources

This is a periodic activity that the ITSM Service Desk launches twice a year based on an ITSM Security Manager’s request (when the process is started at a beginning of a month the ITSM Security Managers use the data obtained in SEC.6.2). ITSM Service Desk provides the user list related to the ITSM SMT. “users” are those individuals who have accounts that allow them to create calls.

The user list is sent under the form of an Excel file; it reflects the current situation. The authoritative source is the user list of the application.

ITSM Infrastructure Management extracts the user details from this source, and exports the user details to Excel workbooks.

The content is:

IT resource	Contents
ITSM SMT	One row per user, containing at least: • Full name – Last name, first name; E-mail address.

SEC.5.7

SM - Collect user details from authoritative sources

SEC.5.7 SM – Collect user details from authoritative sources

This is a periodic activity that an ITSM Security Manager launches twice a year. The ITSM Security Manager collects user lists related to the following ITSM IT resources (when the process is started at a beginning of a month the ITSM Security Managers use the data obtained in SEC.6.4):

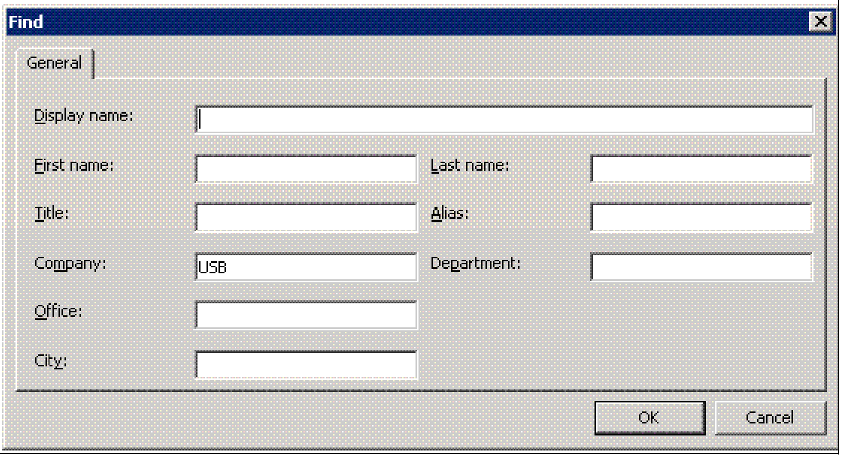
- ITSMTAXUD mailboxes.

The information is collected under the form of an Excel file; it reflects the current situation. The authoritative sources related to each IT resource are listed below:

IT resource	Source
itsmtaxud mailboxes	The address book that is accessible from an Outlook e-mail client connected to the ITSMTAXUD Exchange server.

The ITSM Security Manager extracts the user details of the relevant users by selecting address book records based on the following criteria:

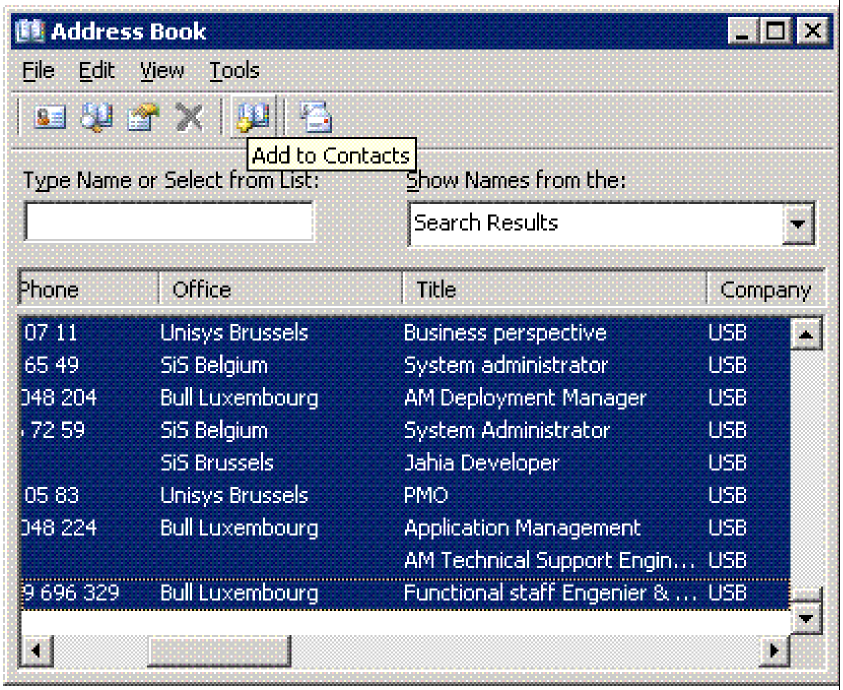
- Mailboxes – Address book records with the “Company” field containing “XXX”. The selection occurs as shown in the screenshot below:



Company: USB

Figure 4-13: ITSMTAXUD mailbox selection

The ITSM Security Manager exports the details of the selected users to Excel workbooks. This is carried out in MS Outlook by momentarily storing selected records in the Contact List as shown in the screenshot below:



Phone	Office	Title	Company
07 11	Unisys Brussels	Business perspective	USB
65 49	SiS Belgium	System administrator	USB
048 204	Bull Luxembourg	AM Deployment Manager	USB
72 59	SiS Belgium	System Administrator	USB
	SiS Brussels	Jahia Developer	USB
05 83	Unisys Brussels	PMO	USB
048 224	Bull Luxembourg	Application Management	USB
		AM Technical Support Engin...	USB
9 696 329	Bull Luxembourg	Functional staff Engenier & ...	USB

Figure 4-14: Collect ITSMTAXUD mailboxes

The Contact list is then exported to an Excel file; the content is:

IT resource	**Contents**
itsmtaxud mailboxes	One row per user, containing at least: • Full name – Last name, First name; E-mail address.

SEC.5.8

Compare user lists with authorised user list

SEC.5.8 Compare user lists with authorised user list

For each XXX team, the ITSM Security Manager makes a list of XXX users that are present in a user list but absent of the authorised user list (Annex 4 of MPR).

SEC.5.9

Check the lists of users to revoke with ILSOs

SEC.5.9 Check the lists of users to revoke with ILSOs

The ITSM Security Manager sends each list of XXX users that are not in the authorised user list to the ILSO of the team. The ILSOs check that the users of the lists do not work anymore on ITSM and send the confirmation to ITSM Security Management. Then the ITSM Security Manager sends the list of users who were not identified by the ILSOs to the Projects

	directors for a final confirmation. When ITSM Security Management has received all the answers of the Projects directors, the ITSM Security Manager sends an E-mail to ITSM Service Desk requesting the revocation of the relevant users. The ITSM Security Manager submits the result of the review to the ITSM Service Level Management (WP.8.2.1) for bundling into the current month's MPR.
SEC.5.10 Request the CCN user lists to CCN/TC	**SEC.5.10 Request the CCN user lists to CCN/TC** ITSM Security Manager requests to CCN/TC the user lists related to CCN. The information is sent under the form of one CSV file per gateway; it reflects the current situation as listed below: One row per user per profile, containing at least: • User – The ID of the user account; • Profile – The profile owned by the user; • User info – The free text description about the user; • User aging – When CCN/TC tools will allow it, the date of last use of this profile by the user.
SEC.5.11 Process user lists	**SEC.5.11 Process user lists** When the lists are delivered, the ITSM Security Manager processes the delivered lists as follows: • Import the CSV files into Excel; • Remove useless information. Only the content that is described in the step below remains; • Add a column named "Change D/K" (Disable/Keep) for completion by the Local Security Administrators with the new status; • Protects the data (except the column "Change D/K") to prevent the NPMs from updating the wrong cells. The protection password is blank.
SEC.5.12 Send the e-mails to the Local Security Administrators	**SEC.5.12 Send the e-mails to the Local Security Administrators** • For each gateway, the ITSM Security Manager prepares an e-mail with the processed UAM file in attachment. These e-mails ask the Local Security Administrators (note: the LSA details are provided by the ITSM Service Desk) to review

the users rights and remove the profile of the users that do not need them anymore. When the user profiles have been updated, it is asked to the Local Security Administrator to update the “Change D/K” column in the UAM file and to send back the updated UAM file to the ITSM Service Desk (for information). It is the LSA role to actually remove the user; the LSAs send a signed form to ITSM Security Management to confirm that they actually did the remove;

- The ITSM Service Desk sends the prepared e-mails to the Local Security Administrators (who manage the CCN gateways);

- Before attaching the e-mails to the incident on ITSM SMT, the ITSM Service Desk removes the Excel sheets (for confidentiality reasons, as it is accessible through the ITSM Webportal);

- After two weeks, the ITSM Service Desk sends a reminder to the Local Security Administrators that have not yet replied;

- Two weeks later, the ITSM Service Desk sends a reminder to the Local Security Administrators that still have not yet replied.

SEC.5.13

Consolidate the UAM files

SEC.5.13 Consolidate the UAM files

- On receipt of an e-mail from Local Security Administrators, the ITSM Service Desk forwards the complete answers to the ITSM Security Management;

- Before attaching the e-mails to the incident on ITSM SMT, the ITSM Service Desk removes the Excel sheets (for confidentiality reasons, as it is accessible through ITSM Webportal);

- The ITSM Security Manager consolidates the result of the review and submits it to the ITSM Service Level Management (WP.8.2.1) for bundling into the current month’s MPR.

SEC.5.14

Send the e-mails to the IGLs

SEC.5.14 Send the e-mails to the IGLs

- The ITSM Security Manager informs the DG TAXUD CIRCA Administrator (TAXUD-CIRCA-ADMIN@ec.europa.eu) that a review will be performed; he asks the DG TAXUD CIRCA Administrator (TAXUD-CIRCA-ADMIN@ec.europa.eu) to provide a fresh list of Interest Group Leaders (i.e., those individuals at DG

TAXUD who are in charge of managing the accesses to a CIRCA Interest Group);

- The ITSM Security Manager prepares an e-mail by editing a copy of the e-mail formatted for CIRCA review (at the moment of the FQP delivery, it is located on ITSM Collaborative Tool under: "*Browse » Folders » ITSM Project (XXX) » 04. Security Management » CIRCA user access review » Bi-annual review of user accesses. zip*");
- ITSM Service Desk sends the e-mail to the Interest Group Leaders (the e-mail addresses are put in BCC);
- After two weeks, ITSM Service Desk sends a reminder to the Interest Group Leaders that have not yet replied;
- Two weeks later, ITSM Service Desk sends a reminder to the Interest Group Leaders that have still not yet replied.

SEC.5.15

Submit the result of the review

SEC.5.15 Submit the result of the review

- On receipt of an e-mail from IGLs, the ITSM Service Desk forwards the complete answers to ITSM Security Management;
- The ITSM Security Manager consolidates the result of the review and submits it to the ITSM Service Level Management (WP.8.2.1) for bundling into the current month's MPR.

SEC.6.1

INFRA - Collect user details from authoritative sources

SEC.6 User List Management

SEC.6.1 INFRA – Collect user details from authoritative sources

This is a monthly activity that the ITSM Infrastructure Management launches on the first w-day of the month. It consists in the provision of user lists and of joiners/leavers lists to the ITSM Security Management.

User lists – ITSM Infrastructure Management provides user lists related to the following ITSM IT resources:

- ITSM Collaborative Tool;
- ITSM VPN.

The information is sent under the form of an Excel file; it reflects the situation at the end of the previous month. The authoritative sources related to each IT resource are listed below:

IT resource	Source

ITSM Collaborative Tool	The user list of the application.
VPN	An Excel workbook, which is maintained by ITSM Infrastructure Management on a day-to-day basis.

The ITSM Infrastructure Management extracts the user details from these sources, and exports the user details to Excel workbooks when the source is not itself an Excel workbook.

The content is:

IT resource	**Contents**
ITSM Collaborative Tool	One row per user, containing at least: • Full name – Last name, First name; Userid – The first 4 characters of a userid are “XXX.” (For XXX team members), “txd.” (For DG TAXUD), or “lot.” (For non-ITSM contractors). Userids that start neither with “XXX.”, “txd.”, nor with “lot.” refer to support users (e.g., the ITSM COLLABORATIVE TOOL administrator) or to disabled ones.
VPN	One row per user, containing at least: • Full name – Last name, first name; Active Y/N – Contents is “Y” for active VPN connexions; it is “N” for inactive ones.

Joiners/leavers – In addition to the user lists, ITSM Infrastructure Management provides the list of XXX team members who have either joined or left the team during the last month. It is an Excel workbook that ITSM Infrastructure Management maintains on a daily basis. It contains one worksheet per month. A row in a worksheet concerns one user and contains at least the following information:

- Full name – Last name, First name;
- Status – Values are: “Disabled” or “Created”;
- Rights – For a “Created” user, it indicates which access rights to the IT resources that are managed by ITSM Infrastructure Management (i.e., ITSM network, ITSM mailbox, ITSM COLLABORATIVE TOOL, JIRA, and/or VPN) have been granted to the user.

SEC.6.2
SD - Collect user details from authoritative sources

SEC.6.2 SD – Collect user details from authoritative sources

This is a monthly activity that the ITSM Service Desk launches on the first w-day of the month. The ITSM Service Desk provides the user lists related to the following ITSM IT resources:

- The ITSM Webportal;

- The ITSM SMT Service Management Tool.

The information is sent under the form of an Excel file; it reflects the situation at the end of the previous month. The authoritative sources related to each IT resource are listed below:

IT resource	Source
ITSM Webportal	The database of the ITSM Webportal user management tool.
ITSM SMT	The user list of the application.

ITSM Infrastructure Management extracts the user details from these sources, and exports the user details to Excel workbooks. The contents are:

IT resource **Contents**

ITSM Webportal One row per user, containing at least:

- Full name – Last name, First name;
- Organisation – The organisation (NA, Commission, contractor…) the user is working with;
- CS/RD Domain – CS/RD domains that are accessible by the user: NCTS, ECS, ICS and/or EO;
- CS/RD TST – Rights on CS/RD test domain: it is either empty, or it contains “Full”, “No”, “Read” or “Write”;
- CS/RD PROD – Rights on CS/RD production domain: it is either empty, or it contains “Full”, “No”, “Read” or “Write”;
- CS/MIS Domain – CS/MIS domains that are accessible by the user. The values are:

Value	Domains
E	ECS
I	ICS
N or NCTS	NCTS
EI	ECS and ICS
EN	ECS and NCTS
IN	ICS and NCTS
EIN or B	ECS, ICS and NCTS

Deleted – “FALSE” if the user is still active; “TRUE” otherwise.

ITSM SMT One row per user, containing at least:

- Full name – Last name, First name;
- E-mail address.

SEC.6.3
AM - Collect user count from authoritative sources

SEC.6.3 AM – Collect user count from authoritative source

This is a monthly activity that ITSM Application Management launches on the first w-day of the month. ITSM Application Management provides the amount of registered user in a series of DG TAXUD's business applications. On 01/01/2010, the list of concerned applications is as follows:

- AEO;
- ART;
- CN;
- CMR;
- EBTI;
- ECICS2;
- EOS;
- ISPP;
- QUOTA;
- QUOTA2;
- RIF;
- SMS;
- SURV2;
- SUSPENSIONS;
- TARIC.

The list above may vary every month according to the set of business applications ITSM Application Management is managing.

The authoritative source is the WebLogic console.

SEC.6.4
SM - Collect user details from authoritative sources

SEC.6.4 SM – Collect user details from authoritative sources

This is a monthly activity that an ITSM Security Manager launches on the first w-day of the month. The ITSM Security Manager collects user lists related to the following ITSM IT resources:

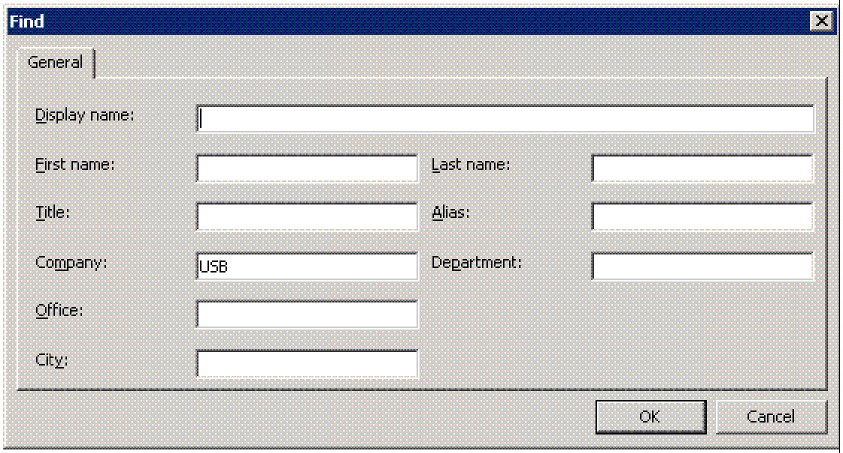
- The ITSMTAXUD mailboxes.

The information is collected under the form of Excel files; it reflects the situation at the end of the previous month. The authoritative sources related to each IT resource are listed below:

IT resource	**Source**
itsmtaxud mailboxes	The address book that is accessible from an Outlook e-mail client connected to the ITSMTAXUD Exchange server.

The ITSM Security Manager extracts the user details of the relevant users by selecting address book records based on the following criteria:

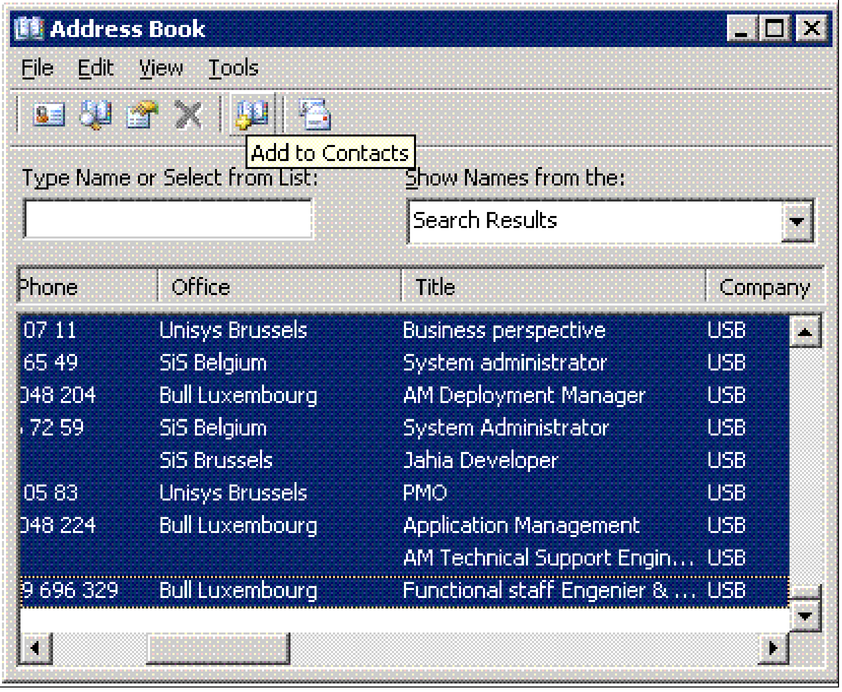
- Mailboxes – Address book records with the “Company” field containing “XXX”. The selection occurs as shown in the screenshot below:



Company: USB

Figure 4-15: ITSMTAXUD mailbox selection

The ITSM Security Manager exports the details of the selected users to Excel workbooks. This is carried out in Outlook by momentarily storing selected records in the Contact List as shown in the screenshot below:



Show Names from the: Search Results

Phone	Office	Title	Company
07 11	Unisys Brussels	Business perspective	USB
65 49	SiS Belgium	System administrator	USB
48 204	Bull Luxembourg	AM Deployment Manager	USB
72 59	SiS Belgium	System Administrator	USB
	SiS Brussels	Jahia Developer	USB
05 83	Unisys Brussels	PMO	USB
48 224	Bull Luxembourg	Application Management	USB
		AM Technical Support Engin…	USB
9 696 329	Bull Luxembourg	Functional staff Engenier & …	USB

Figure 4-16: Collect ITSMTAXUD mailboxes

The Contact list is then exported to an Excel file; the contents are:

IT resource	**Contents**
itsmtaxud mailboxes	One row per user, containing at least: • Full name – Last name, First name; E-mail address.

SEC.6.5

Process collected user lists

SEC.6.5 Process collected user lists

When the lists described in the SEC.6.1, SEC.6.2, SEC.6.3 and SEC.6.4 steps are delivered, the ITSM Security Manager processes as follows:

- All lists
  - When needed, remove useless information. Only the contents that are described in the steps SEC.6.1, SEC.6.2, SEC.6.3 and SEC.6.4 remains (note: some user lists contain information that is useless in this context, e.g., phone numbers or postal address);
  - When needed, ignore disabled users (note: in some lists —ITSM Webportal, ITSM SMT— a user record is never deleted; it is flagged as disabled).
- List of ITSM SMT users
  - Remove duplicates. The removal relies on a comparison of e-mail addresses (note: duplicates happen when users subscribe to the service using different spellings in their name);
  - Make a separation between records related to ITSM staff on one hand, and to other users (European Commission, non-ITSM contractors, and NA representatives) on the other hand. The process relies on the domain names in the e-mail addresses.
- ITSMTAXUD mailboxes
  - Make a separation between records related to nominative mailboxes on the one hand, and to non-nominatives ones on the other hand. The process relies on an analysis of the users' full names.
- Other lists: ITSM Webportal, ITSM Collaborative Tool, VPN, business applications, joiners/leavers lists
  - No further processing needed.

When necessary the processing as described above is implemented as a VBA script.

SEC.6.6

Generate report including counts of managed users

SEC.6.6 Generate report including counts of managed users

The lists processed as described in SEC.6.5 are grouped as worksheets in one Excel workbook (filename ends with “User List.xls”). One extra worksheet is added with the counts; contents are:

- Amount of managed users in business applications;
- ITSM Webportal users:
  - Total amount of managed users;
  - Amount of users without access rights to NCTS, ECS, ICS;
  - Amount of users having access rights to NCTS, ECS, ICS;
  - Amount of users without access rights to CS/RD TST;
  - Amount of users having access rights to CS/RD TST;
  - Amount of users without access rights to CS/RD PROD;
  - Amount of users having access rights to CS/RD PROD;
  - Amount of users without access to a CS/MIS domain;
  - Amount of users having access rights to a CS/MIS domain;
  - Amount of users without a CS/MIS profile;
  - Amount of users having a CS/MIS profile;
- ITSM SMT users:
  - Total amount of managed users;
  - ITSM users;
  - Non-ITSM users;
- ITSMTAXUD mailboxes:
  - Total amount of managed users;
  - Amount of nominative mailboxes;
  - Amount of non-nominative mailboxes;
- ITSM Collaborative Tool:
  - Amount of nominative accounts;
  - Amount of non-nominative accounts;
- VPN:
  - Total amount of managed users.

Moreover the average of the figures above on a three-month

	sliding window is added. The average values are rounded to the nearest unit. Three-month averages are provided when the history is sufficient, i.e., after 3 months of process execution. The resulting worksheet is submitted to Service Level Management (WP.8.2.1) for bundling into the current month's MSR.