# CUSTOMS INFORMATION SYSTEM

Report of the Joint Supervisory Authority of Customs presenting a general overview of the use of the Customs Information System by the Member States.

**Brussels, 18 December 2007**

## Contents

## I. Introduction

On request of the Customs Joint Supervisory Authority (further referred as JSA), the national data protection authorities asked the competent authorities of their state to report on the security measures applied in the Customs Information System (further referred as CIS). In this report the JSA presents the findings of these national surveys.

In May 2006, the JSA instructed the Data Protection Secretariat to report on the information security infrastructure and the related procedures of the CIS. ?he Data Protection Secretariat visited the European Anti-Fraud Office (further referred as OLAF) in Brussels, which is responsible for the technical implementation, management and maintenance of the CIS. The scope of the visit was to report on the technical infrastructure and the security measures laid down by OLAF for the CIS.

The findings of this visit were discussed by the JSA in June 2006. Based on this report and some general statistics on the usage of the CIS, the JSA decided to start this survey concerning the security measures applied for the CIS by the national competent authorities in the Member States. The JSA envisaged in 2006 that the findings of this joint report would be useful for the first inspection to the central system in OLAF.

In 2007, the JSA used these findings for the preparation of the inspection in the central CIS. An inspection team composed by national experts was appointed. The Data Protection Secretariat organized the first inspection in the CIS 3rd Pillar that took place in June 2007 in OLAF. The JSA is very pleased to present this report at the same time with the inspection report. The JSA would also like to thank all the national authorities who contributed to this report.

## II. Data Protection Supervision

The legal framework of the Customs Information System (CIS) is based on a Council Regulation[1] and the Convention[2]. The CIS was created to store information on commodities, means of transport, persons and companies in order to assist in preventing, investigating and prosecuting actions which are in breach of customs and agricultural legislation (1st Pillar) or serious contraventions of national laws in the application of which the customs administrations have total or partial competence (3rd Pillar).

The aim of the Customs Information System, as defined in the legal basis, is to create an alert system in the framework of the fight against fraud and to enable a Member State which inputs data into the system to request another Member State to carry out one of the following actions:

–sighting and reporting,

–discreet surveillance, or

–a specific check.

Following the provisions of the CIS Convention, personal data are processed in the CIS by the Member States. The CIS Convention divides the data protection supervision on the content and the functioning of the CIS between national data protection authorities and the JSA. The Member States are responsible for the processing of personal data in the CIS according to the CIS Convention and they are supervised by the national Data Protection Authorities. The JSA has the overall task to supervise the technical support function of the CIS. This function is responsible for distributing the data entered in the CIS to all Member States.

Article 18 of the CIS Convention describes the tasks of the JSA. Apart from checking the operation of the CIS, the JSA is charged with examining any difficulties of application or interpretation that may arise with the operation of the SIS, as well as drawing up harmonized proposals for joint solutions to existing problems. These are the basic legal grounds for initiating an inspection of the operation of the CIS with particular to the applied security measures.

[1] Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of law on customs and agricultural matters (OJ L 82, 22.3.1997, p. 1).

[2] Convention drawn up on the basis of Article K.3 of the Treaty on European Union on the use of information technology for customs purposes of 26 July 1995 (OJ C 316, 27.11.1995, p. 34)

## III. Scope and method of inspection

Before initiating this survey the JSA defined the main objective and the method. The objective of this survey was to check if security measures proposed by OLAF concerning the use of the CIS 3rd Pillar are being applied by the national competent authorities in a consistent way. The method of the survey would also make the JSA able to assess whether any problems exists as to the operation of the CIS.

To that purpose the JSA adopted a simple method of inspection to be used equally by all national Data Protection Authorities. The use of this model could enable the JSA to compare results and evaluate the differences between the Member States.

The Data Protection Secretariat developed a comprehensive questionnaire (see annex) which was sent to the national Data Protection Authorities in July 2006. The questionnaire aimed to get an overview of the applied security measures on a national level.

Some Member States made on site inspections using this questionnaire, while others simply sent the questionnaire to the responsible national authorities for completion.

## IV. Reactions received

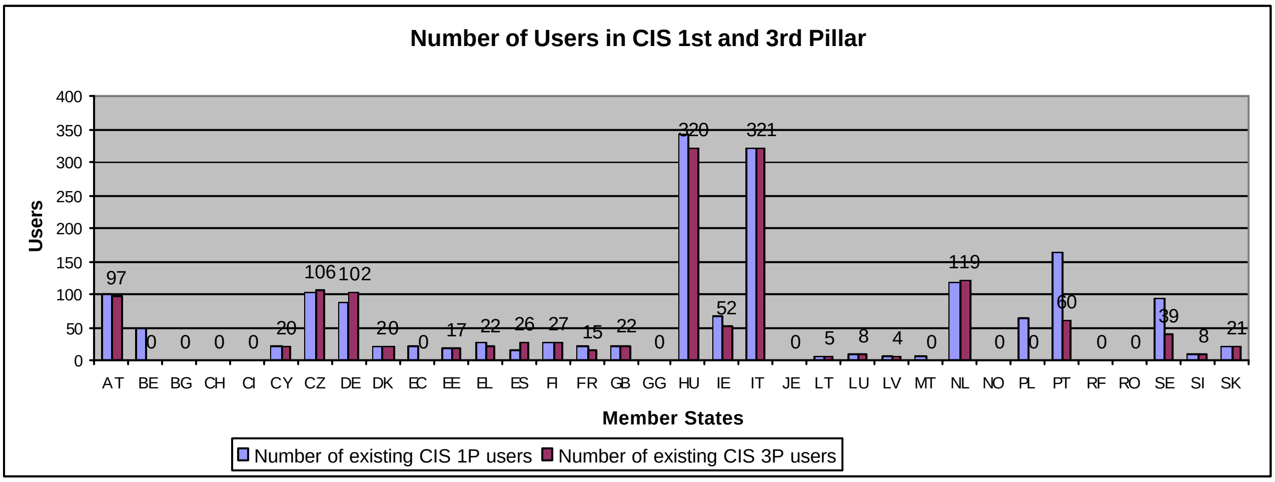
Nineteen (19) data protection authorities in the Member States have participated in this survey: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Slovakia, Slovenia and Sweden. All of them provided the JSA Customs with comprehensive information on the usage of the Customs Information System.

Apart from the answers to the questions, some Member States also sent additional remarks. For example, Cyprus reported that the system is not used very often because of the usage difficulties and the fact that only a small amount of data is currently processed. Poland, noted that for comprehensive examination of the problems it would be essential to conduct inspections in the customs chambers. These inspections will be included in their future inspection plan. A very positive outcome of this survey is noted in Lithuania. There, the inspection revealed a number of security problems in the usage of the CIS system. Following that, the Data Protection Authority requested their national Customs Authorities to take action for solving these problems. A follow-up inspection ensured that the recommendations were implemented by the Customs authorities.

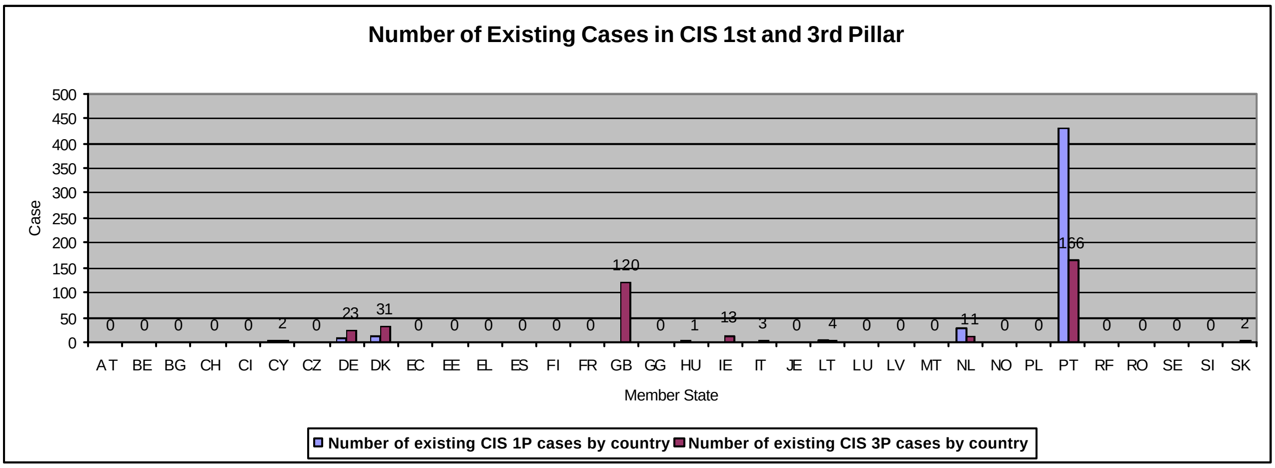
## V. Statistics of the CIS content

Before presenting the findings of the survey, an overview of the current content of the CIS provides significant information on the real usage of the CIS by the Member States. The aforementioned statistics refer to May 2007. A detailed overview was provided by OLAF to the Data Protection Secretariat.

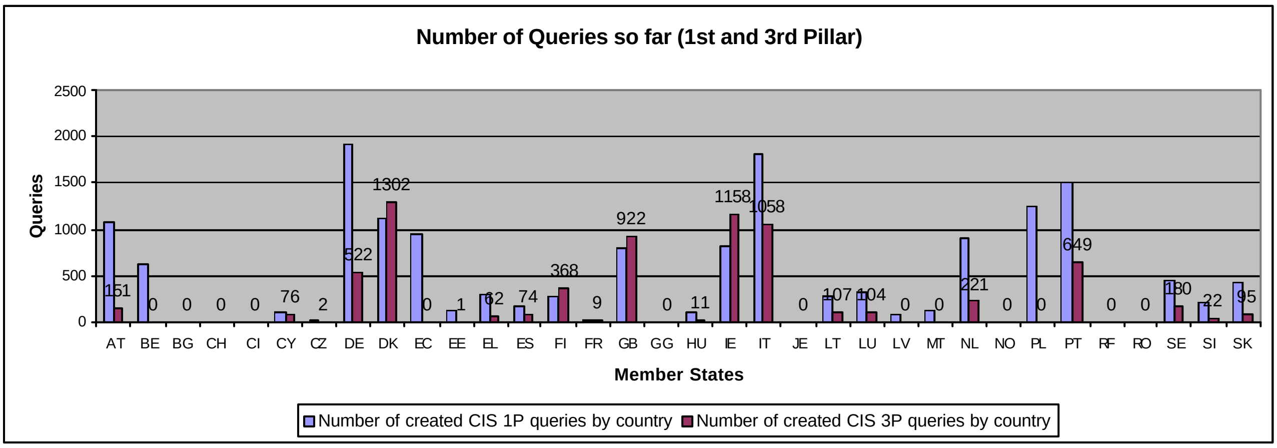
As shown in the next tables, the CIS is not used very much by the Member States. One of the explanations given is that the current version of CIS is not very user friendly and there are many time delays in the system responses to users' requests from the Member States.



Although the number of users is huge, not many cases are active in CIS 3rd Pillar, as shown in the following table.



In the 3rd Pillar most of the active cases have been entered by Portugal (166 cases) and UK (120 cases). Most of the users are found in Italy (321) and Hungary (320 users).



As on 31st May 2007 there were:

- 1431 third pillar active (“existing”) users
- 376 third pillar active cases,
- 7094 third pillar queries

All these numbers following the results of this survey provided to the JSA important feedback for the preparation of the inspection. For example the extensive number of users in a system that has not been used very much, was an indication that a problem of the user management procedures existed. This matter is also dealt with in this report.

In the following section the results of the survey are presented.

## VI. Results and evaluation

### 1. INFORMATION SECURITY CO-ORDINATION

In June 2006 the Data Protection Secretariat reported to the JSA that OLAF did not yet distributed the approved Security Policy for the CIS. However, the CIS (1st and 3rd Pillar) Operating Procedures Manual, which was issued in October 2002 and used by the Member States, contained a paragraph on security. This paragraph described basic principles and minimum security standards which Member States and the Commission should apply.

OLAF issued the AFIS Security Policy document in May 2006. This document recorded the Security Policy for the set of applications collectively known as the Antifraud Information System (AFIS), which also includes the CIS. It provided guidelines for the development of specific policies, and to ensure a common understanding by all Member States and the Commission on security responsibilities and requirements. The implementation of the AFIS Security Policy is recommended to the Member States by OLAF.

*The Member States*[3] *were asked to answer whether their national desks had applied a security policy for CIS and whether there where any security activities that were in compliance with the security policy proposed by OLAF. They were also asked to assess whether the applied security controls are adequate and coordinated and whether the competent CIS authorities have contacted any education lectures on security matters, training etc.*

The answers to this question indicated that almost all Member States apply security policies and procedures. Some of them use existing policies, measures and guidelines that were available for their other systems beforehand while others have adopted the same security policies that were proposed by OLAF. In the Netherlands a security policy is not yet available as the system is not yet fully used. In Poland however it was noted that OLAF has not yet provided them with the AFIS Security Policy.

These findings show that different security policies are applied by the Member States for the CIS. This could mean that the security standards that are followed might not provide the same level of security. Such situations can compromise the security of the system. However, this issue has to be evaluated as all the Member States reported that the security measures are generally in compliance with the security rules proposed by OLAF, that they are adequate and coordinated (except Belgium where the security controls are not yet systematic) and in some cases even more strict (like Hungary) rules are applied.

In view of this, the implementation of a common document on the Security Policy for CIS (as the AFIS Security Policy), is recommended.

All Member States also reported that training is essential and that several training courses were done in the areas of IT safety and courses in accordance with the CIS procedures.

### 2. ROLES AND RESPONSIBILITIES

*The Member States were asked to report whether their competent authorities for CIS have oriented a security role(s) for the system and documented in accordance with their security policy.*

All, except Belgium, answered positively to this question. Some provided more clear answers explicitly saying that a security officer is appointed for the CIS.

The Member States where also asked to describe the functions of the security role(s) in particular to: a) the implementing and acting in accordance with the security policy; b) protection of assets from unauthorized access, disclosure, modification, destruction or interference; c) execution

[3] The reference Member States regards those Member States that participated in the survey.

of particular security processes or activities; d) ensuring for granting responsibilities to certain actions; e) reporting of security events or potential events or other security risks to the national responsible authority for CIS.

All of them answer positively to the questions except Greece and Luxembourg that answered negative to the c) and e) topic and to the c) topic respectively.

## 3. INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING.

*All employees of the national responsible authority for CIS should have received appropriate awareness training and regular updates in CIS policies and procedures, relevant to their job function. Training to enhance awareness is intended to help users recognize information security problems and incidents, and respond according to the needs of their working` role.*

Almost all the Members States initiated training as proposed in the CIS Manual. National trainers were educated by OLAF (answers from Austria, Latvia, Lithuania, Slovakia, Slovenia and Sweden) who then conducted the training in their national units. In the Netherlands training is still on-going. In Belgium training has not yet started. All answers confirmed that training was necessary for all CIS users.

## 4. REMOVAL OF ACCESS RIGHTS

*The access rights of the users to CIS should be removed upon not usage of the system, termination of their employment, or adjusted upon change. The Member States were asked to report if the national responsible authority for CIS maintains a users access control diagram and if they control the actual usage of the system and removes user accounts in cases of not usage.*

In June 2006, OLAF did not have developed a user management procedure. One of their main problems, mentioned to the Data Protection Secretariat, was that there were many users registered in the system[4] without really using it. The followed best practice is that access rights of users to CIS should be removed upon not usage of the system, termination of their employment, or adjusted upon change.

For this purpose, OLAF planned to develop a user management procedure and a technical measure, where, not active users for a long time will be automatically deleted from the system. In principal, the Member States are responsible for the creation of the users.

All the Member States, except Austria and Greece, reported that they maintain an updated user's access control diagram. This diagram lists the users and their access rights. Sweden reported that they ask for logs from OLAF to check on the system usage.

As to the actual usage of the system, all the Member States except Belgium, Hungary and Sweden do periodical controls and they ask for the deletion of inactive users. Especially, for Hungary where a big number of users are registered this has to be better controlled. Member States must delete inactive users and communicate this need to OLAF.

## 5. PHYSICAL AND ENVIRONMENTAL SECURITY

*The Member States were asked to report if the CIS terminals and the CIS hardware facilities are physically protected from unauthorized access, damage, and interference.*

The CIS terminals must be physically protected from unauthorized access, damage, and interference. All gave positive answers to this aspect. Hungary and Poland, for example have a security increased zone. Sweden, also implemented security measures with smart cards. The areas of the CIS hardware facilities are adequately protected by appropriate entry controls ensuring that

[4] For example in June 2006 Hungary had 305 active users while in May 2007 320 users.

only authorized personnel are allowed access. Most of the Member States already applied physical security measures on their offices. In Lithuania however, it was reported that in the first inspection not all offices were adequately physically protected. After their recommendations this was improved.

## 6. CONTROLS AGAINST MALICIOUS CODE

*The Member States were asked to report if the computer, where the CIS is installed, has access to the Internet. Additionally if there is a formal policy a) prohibiting the use of unauthorized software; b) protecting against risks associated with obtaining files and software either from or via external networks, or on any other medium.*

The computers with a CIS terminal in Austria, Belgium, Cyprus, Denmark, Estonia, Finland, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Netherlands[5] and Sweden have access to Internet but special technical measures have been taken to prevent any malicious attack. Only in Czech Republic, Greece, Italy, Poland, Slovakia and Slovenia the CIS terminals have no access to Internet. All national competent authorities for CIS in every Member State applied the aforementioned formal policy on controls against malicious codes.

## 7. MONITORING

*The Member States were asked to report on whether they monitor the usage by checking audit logs and/or having an audit policy.*

Enabling security auditing and viewing the security logs is important for the security of the CIS. As Member States are responsible for the content of the CIS, its use should be monitored on a national level. It is noted, that in the AFIS Security Policy there are no procedures for auditing data. OLAF does not provide the Member States with an audit tool. Only upon request, the database administrators in OLAF can send audit logs to a Member State. It was also reported, that until now only two requests of audit logs where made to OLAF by the Member States and one of those was triggered by this survey.

Different answers were provided to this aspect. Austria, Belgium, Denmark, Greece, Hungary, Ireland, Latvia, Luxembourg, Netherlands, Poland, Slovakia, and Slovenia responded that monitoring on a national level is technically impossible thus confirming that only OLAF can produce audit logs. The Czech Republic, Cyprus, Estonia, Finland, Lithuania and Sweden answered that they have audit logs in place recording user activities. In Italy this is done partly.

An audit policy is in place in Czech Republic, Estonia, Slovakia and Slovenia. Finland is preparing an audit policy while Sweden expects the new regulations.

Monitoring of the system is always a critical point. Regarding CIS, it is concluded that a technical issue exists, as no audit facilities are provided to the Member States for monitoring and control and it is also evident that also OLAF do not execute any monitoring activities. Since the answers on this question seem sometimes contradictory with the findings of the JSA in respect of the functioning of CIS, a further examination of this issue is needed.

[5] Only for specific url's- see page 18.

## 8. ACCESS CONTROL POLICY

*The Member States were asked to report if there is an access control policy established, documented, and reviewed based on the CIS manual. And if yes, that there are access control rules and rights for each user or group of users clearly stated.*

Almost all the Member States declared that they have an access control policy based on the CIS manual. This access control policy defines in all Member States (*except Belgium, Cyprus*) the access control rules and rights for each user or group of users. An access control policy should be equally adopted in all Member States.

## 9. USER ACCESS MANAGEMENT

*The Member States were asked to report if there are any formal procedures to control the allocation of access rights to the CIS and if these procedures cover all stages in the life-cycle of user access.*

The Member States are responsible for the creation of the users. This is done via a special form signed by the "Authorizer" which is sent to OLAF. OLAF then creates the users and sends back information to the "Authorizer". Formal procedures have been adopted by almost all Member States (*except Belgium*) to control the allocation of access rights to the CIS.

Only Belgium and Luxembourg do not have procedures that cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to the CIS.

## 10. USER REGISTRATION

*The Member States were asked to report if they have in place a formal user registration and de-registration procedure for granting and revoking access to the CIS.*

Only Austria and Belgium did not confirm the existence of such a procedure. However Austria's answer reports the use of a standard workflow that can be deemed as a procedure.

## 11. USER PASSWORD MANAGEMENT

*The Member States were asked to report if the allocation of passwords is controlled through a formal management process, if there is a password policy applied for CIS in a national level and if the users have been trained to follow good security practices in the selection and use of passwords.*

Almost all Member States confirmed that the allocation of passwords is controlled through a formal management process. OLAF describes some rules for choosing strong passwords in the document "Procedures Manual" but it is up to the Member State to apply a good password policy. OLAF informed the Data Protection Secretariat that the CIS users do not choose secure passwords and that the system cannot technically enforce selection of strong passwords. On the other hand, all the Member States confirmed that all users are trained to follow good security practices in the selection and use of the passwords and that a password policy has been developed on a national level. However in Belgium for example this is done verbally. This area needs further investigation.

### 12. REVIEW OF USER ACCESS RIGHTS

*The Member States were asked to report if the responsible authority for CIS review users' access rights to CIS at regular intervals (e.g. a period of 6 months, and after any changes, such as promotion, demotion, or termination of employment) using a formal process.*

All Member States confirmed that the responsible authority for CIS reviews users' access rights to CIS at regular intervals (e.g. a period of 6 months, and after any changes, such as promotion, demotion, or termination of employment) using a formal process. For example, in Hungary the period is chosen randomly, in Ireland this only takes place when changes in staff occur, in Austria on average one per year quarter, in Slovakia every six months. The practice does not follow common rules but the national security policies.

## VII. **Conclusions**

The JSA presented the findings of the survey on the security practices applied for CIS by the national competent authorities. In general the answers support the implementation of security measures concerning the CIS although these measures are different between the Member States.

From the answers that were received together with the findings of the inspection report some areas have to be improved. It is obvious that the management of the users is not done systematically by the Member States. A very important issue is the lack of monitoring of the system. No audit policy or any technical tool is available for this purpose. Member States should be provided with a technical solution for monitoring the use of the CIS on national level. A password policy guaranteeing the use of robust passwords must be better enforced by Member States. The JSA therefore proposes that the Member States should also evaluate whether the CIS computers that have connection with the Internet introduce any security risks. It is suggested that a specific CIS security policy is applied by all Member States providing at least a level of security equal to the AFIS Security Policy.

The JSA hopes that the results of this survey along with the inspection report will guide OLAF and the Member States to further improve the security and management of the CIS.

# Annexes

## Received Answers

In this section the detailed answers that were received by the Member States are presented.

### 1. INFORMATION SECURITY CO-ORDINATION

Typically, the information security proposed by OLAF should be followed by the responsible for the CIS national authority.

1.1. Has the national desk applied a security policy for the CIS?

| | |
|---|---|
| **Austria**[6] | No, there isn't a specific national security policy for the CIS; but there are, however, instructions and guidelines to comparable national databases in force which comply with the high safety standards of the CIS (national data protection law, Austrian tax law, data security regulation for the tax and customs administration, information-security roles for IT and in the Austrian tax and customs administration, guidelines for IT security, safety guideline for the use of internet, guideline for the use of e-mails, individual access regulations for the Ministry of Finance and local offices, annual instructions about data protection regulations etc.) |
| **Belgium** | No. The national desk has not applied a security police for the CIS. However, as far as possible and taking into account the circumstances, they apply the rules as proposed in the OLAF document "Customs information system (CIS) – Security rules" (Bruxelles, 035521 * 05.04.2002, DG/TH D(2002) ) |
| **Czech Republic** | Yes – the security policy is laid down in the Service Instruction on Customs Information System (No. 76/2004). |
| **Cyprus** | All the measures of the security policy proposed by OLAF are applied but no separate policy has been formed. There are also in existence specific instructions either issued by the Department of Customs and Excise or under the Civil Service law concerning the security requirements regarding sensitive information in general. |
| **Denmark** | Yes |
| **Estonia** | We have Security Policy which states the security measures and policies for all IT systems, including the CIS. The Security Policy is mandatory to follow for all employees. |
| **Finland** | The Finnish customs administration applies the same security policy to CIS as to other IT-systems of the Customs authorities. |
| **Greece** | We have adopted the AFIS security policy. |
| **Hungary** | There is an Information Safety Regulation (ISR) which applies to all IT databases of HCFG (implicitly the national part of CIS). |
| **Ireland** | Yes. A national CIS security officer has been appointed. Access to offices where CIS terminals are located is restricted to relevant Customs Enforcement personnel assigned to specific work areas. In general terms, the security policy applied relating to CIS is in accordance with Revenue's own policy on "Security of Revenue Personal Computer System" and "Revenue Security and Confidentiality Policy". |
| **Italy** | Yes. |
| **Latvia** | Yes, at this moment several documents that correspond to the IS security policy issues are applied for information system security. Any activities with IS and other external IS resources have to be carried out according to the IS security policy. |
| **Lithuania** | Customs of the Republic of Lithuania (further – Lithuanian Customs) doesn't have a special security policy for CIS, but Customs information security policy includes requirements for all Customs' information systems. Customs information security policy was approved by order 1B-441 of 30 June 2006 of Director General of Customs Department. |
| **Luxembourg** | Yes, the Luxembourg customs administration applies the same security policy for CIS than for the other IT-systems in Luxembourg |
| **Netherlands** | Yes, until the system and legislation is upgraded and changed the access to the system itself is limited to personnel working at the CIC (info desk and Front office, about 15 people). There are two authorizers, which are authorizing any 'locally' stored CIS cases, made by CIS-users. Locally stored CIS-cases are stored on the server in Brussels and can only be seen by authorized personnel of the country. So far only two CIS-cases are entered locally by one of the CIS-users and validated by the CIS-authorizer. Authorizing takes place after evaluating the new CIS case (legislation, appropriate |

[6] In Austria the questionnaire was answered by the Ministry of Finance which is only competent for the 1st Pillar. The Ministry of Interior competent for the 3rd Pillar part of the CIS has according to information from the Ministry of Finance not participated in CIS so far.

| | |
|---|---|
| | actions, checking names of persons and companies).<br>The use of the CIS system will be expanded to other personnel when the new CIS-system is introduced. Personnel is educated one on one in the use of CIS and the legislation. Because of the fact that so far entering data was limited to a select group of people a security policy is not yet available |
| **Poland** | As it was stated in the course of inspection conducted, the Ministry of Finance was not provided with security policy for CIS System proposed by OLAF. In the framework of implementing the CIS system, other document was used "Instruction of operational procedures of CIS". |
| **Slovakia** | Yes. Customs Criminal Office (CCO) as responsible authority of Slovak Customs administration in this issue has approved security policy in accordance with CIS (1st and 3rd Pillar) Operational Procedures Manual. |
| **Slovenia** | Yes in accordance with CIS (1st and 3rd Pillar) Operational Procedures Manual and approved standards of the Customs Administration of the Republic of Slovenia (CARS). |
| **Sweden** | There is no specific security policy but the regulations that have been sent out earlier from Brussels are applied. A new policy document for AFIS/CIS is being developed by OLAF. The Swedish Customs has a general security policy that is applied for all systems. |

1.2 Are the security activities executed in compliance with the information security policy proposed by OLAF?

| | |
|---|---|
| **Austria** | In the opinion of the Austrian Ministry of Finance the safety activities are carried out in compliance with the "information security policy" of OLAF and are covered by national regulations as well as the workflows in the cooperation with OLAF. |
| **Belgium** | The security actions are inspired by the security police proposed in the OLAF document "Customs information system (CIS) – Security rules" (Bruxelles, 035521 * 05.04.2002, DG/TH D(2002) ). |
| **Czech Republic** | Yes. |
| **Cyprus** | Yes |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | The security activities are carried out according to the security policy of the customs administration. The information security policy proposed by OLAF is followed. |
| **Greece** | We follow the 2003 AFIS Security Policy Document (ASPD). We have hot received officially the latest version of ASPD from OLAF |
| **Hungary** | The above mentioned ISR pays regard to the CIS Operational Procedures Manual (CIS Manual). There are some safety regulations which are stricter than the recommendations of CIS Manual. |
| **Ireland** | Yes. |
| **Italy** | Yes. There is full compliance with the OLAF information security policy |
| **Latvia** | Yes, CIS national authority is compliant with OLAF information security policy. |
| **Lithuania** | Yes |
| **Luxembourg** | Yes, in accordance to the IT behavior guidelines from the Central IT department the information security policy proposed by OLAF is respected. |
| **Netherlands** | Yes |
| **Poland** | Actions concerning security measures are taken both on the grounds of the above-mentioned documentation and under general rules existing in the Ministry of Finance. |
| **Slovakia** | Yes. |
| **Slovenia** | Yes. See above. |
| **Sweden** | The Swedish Customs applies the present policy, inter alia concerning physical security and completed education, but has not been able to start applying the new one since it has not yet been decided by the European Commission. |

1.2. Are the security controls adequate and coordinated?

| | |
|---|---|
| **Austria** | In the opinion of the Ministry of Finance the IT security checks are adequate and coordinated. |
| **Belgium** | The security controls are not systematic. Therefore, it is difficult to evaluate their adequacy. There are no coordinated controls. |
| **Czech Republic** | Yes – adequate and co-ordinate security controls are carried out in accordance with the rules given in the document "Security Policies of Customs' Information Systems". |
| **Cyprus** | Yes |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | The IT-security controls are considered to be adequate. |

| | |
|---|---|
| **Greece** | We follow the 2003 AFIS Security Policy Document (ASPD). We have hot received officially the latest version of ASPD from OLAF |
| **Hungary** | The annual security inspection plan covers those elements of safety measures that need to be examined. The designated departments co-operate in the security controls. |
| **Ireland** | Yes. |
| **Italy** | Yes. Security controls are carried out periodically |
| **Latvia** | Yes |
| **Lithuania** | Yes, security controls level is adequate. The Permanent Customs Security Coordination Committee coordinates it. General Customs information security policy, approved by Customs Department Director General order No. 1B-441 of 2006 June 30 "On approval of Lithuanian Customs information security requirements" and CIS exploitation policy, which consists of: Customs Department Director General order No. 1B-69 of 2007 January 26 "On approval of European Union Members States Customs Information System data provision, management and protection order", Customs Department Director General order No. 1B-494 of 2005 July 13 "On approval of main modules of European Commission Anti-Fraud information system AFIS and user registration of European Union Member States Customs Information System CIS order" and Customs Department Director General order No. 1B-101 of 2006 February 20 "On assignment of persons liable for implementation and maintenance of European Commission Anti-Fraud information system AFIS modules in Lithuanian Customs", provide these security measures:<br>• Assignation of personal;<br>• CIS access provision and rescission procedures. |
| **Luxembourg** | Yes, but more strict security controls will be applied after the implementation of the new version of CIS. |
| **Netherlands** | Yes |
| **Poland** | Security checks in the organizational scope are conducted for the CIS system in the scope of current control over the realization of outlines included in the documentation concerning operational procedures of CIS, for instance: access to rooms with terminals of the system is allowed only to persons having a clearance from the OLAF office, monitors on working stations are positioned in a way that disables any outsiders to access data. |
| **Slovakia** | Yes. IT security is safeguard by approved internal rules of Slovak Customs Administrations. Responsible officials are regular educated with the aim to ensure the effective protection and security of dates. |
| **Slovenia** | Yes, since national regulations and CARS standards are in compliance with CIS Manual and with OLAF information security policy. |
| **Sweden** | The Swedish Customs applies its own security policy which is adequate and co-ordinated. |

1.3 Has the organization promoted until now information security education, training and awareness

| | |
|---|---|
| **Austria** | In principle, the officers of the Austrian Tax and Customs administration are aware of the sensibility and the protection of confidential data. This matter is also treated in the area of the training of officers. In the year 2005 representatives of all tax and customs offices (IT coordinators and IT experts) were trained especially in IT safety and were advised to spread the thus acquired knowledge further to the officers of their area, to increase further the awareness for IT safety.<br>Furthermore an annual instruction is carried out about the regulations of the data protection law. The users are also instructed in the course of the AFIS-CIS user trainings.<br>Since the beginning of the year 2006 an e-learning module for self study has been offered to all tax and customs officers in the intranet. It covers IT safety and data protection. |
| **Belgium** | No. The administration of customs and excises has no formal policy. Currently, some officials (those who are member of the research investigations) have an USER-ID. Therefore it can be presumed that these officials are familiar with the processing of sensitive information because of the kind of their work. |
| **Czech Republic** | Yes – in 2004 (during CIS implementation), 3 types of training were undertaken:<br>- coordinators training,<br>- registered users training,<br>- unregistered users training.<br>New users were trained continuously when necessary. |
| **Cyprus** | Yes, apart from the training that each new user receives, there was a training course before they joined the system, another training course for all users in June 2005 and a training course for managers in Feb 2005. |
| **Denmark** | Yes |
| **Estonia** | Yes, we have special training session for new and already working employees which includes also |

| | |
|---|---|
| | security training module. There were multiple mentioned training sessions arranged in 2006. |
| **Finland** | Yes, the security education has been given to all users of CIS. |
| **Greece** | Yes, during the training of the users. |
| **Hungary** | The HCFG regularly organizes educations and retraining. Courses include IT safety and data protection rules emphasizing CIS. Updated documents of the trainings can be found in the intranet. |
| **Ireland** | Yes. |
| **Italy** | Yes. In the framework of the Antifraud training given to the officers working in the local antifraud offices and dealing with the management of the system, a specific section of the class is devoted to the CIS system with particular reference to the aspects related to its usage and to the security issues of the system itself. |
| **Latvia** | Yes |
| **Lithuania** | Yes, by initiative of Interior ministry of Republic of Lithuania, 10 customs officers were train. Also Lithuanian Customs is planning to start distant security training for all officers and employees of it on the beginning of 2007. |
| **Luxembourg** | Yes, in accordance to the IT behaviour guidelines from the Central IT department in Luxembourg |
| **Netherlands** | Yes |
| **Poland** | Education in the scope of information security is a part of trainings organized for the users of information systems used in Customs Service. Up to now there were no inspections conducted aimed to control the transfer of information concerning CIS. The Ministry of Finance controls information security within its area. |
| **Slovakia** | Yes. Responsible officials are regularly educated in accordance with CIS procedures. |
| **Slovenia** | Yes. Responsible officials are educated as provided in yearly plan for education and in accordance with CIS procedures. |
| **Sweden** | Yes. |

## 2. ROLES AND RESPONSIBILITIES

2.1 Is a security role(s) oriented by the national responsible authority for CIS and the responsibilities of this role defined and documented in accordance with the security policy?

| | |
|---|---|
| **Austria** | Yes – a security role for AFIS-CIS is defined and OLAF was provided the name of the responsible officer. |
| **Belgium** | The roles for the security management have not been defined by the administration of customs and excises |
| **Czech Republic** | Yes – the security roles are defined according to a position:<br>a)coordinator – guarantees transmitting of all information relevant to the CIS implementation between the Czech Republic and the European Commission,<br>b)CIS project manager – guarantees implementation of all CIS measures in the Czech Republic,<br>c)IT manager – is responsible for technical functionality of CIS in the Czech Republic,<br>d)contact officer – forwards registered users' forms to the OLAF, keeps the register of users in the Czech Republic and CIS technical equipment register,<br>e)approve officer – decides on entry of data to the CIS, provides entry of data from an local database to the CIS central database, gives a notice to the users concerning expiry of one year period for data retention in the CIS,<br>f)advisor – provides training of CIS users. |
| **Cyprus** | The security roles have been specified by the Department of Customs and Excise and the responsibilities of these roles have been defined and sent to OLAF since 2003 |
| **Denmark** | Yes. SKAT has produced a policy on security, which constitute the frame of security on the location of SKAT and the security regarding the electronic communication with third parties. The security policy is a result of the common level of protection which is appointed by OLAF. Furthermore some employees are appointed to have the responsibility for the different aspects of the security related to the use of CIS. |
| **Estonia** | Yes |
| **Finland** | The responsibilities are included in the security policy of the customs administration. |
| **Greece** | Yes. |
| **Hungary** | Yes, the responsibilities of security roles are defined and documented in the ISR |
| **Ireland** | Yes. |
| **Italy** | Yes. There is a security structure in charge of issuing of rules and security policies. |
| **Latvia** | Yes, there are issues about IS user responsibilities and the SRS duties regarding each IS response that is used by the SRS documented within the SRS IS security policy documents |

| | |
|---|---|
| **Lithuania** | According to Customs Department Director General order No. 1B-101 of 2006 February 20 there are assigned following CIS management roles:<br>• Liaison officer;<br>• Officer liable for first pillar;<br>• Officer liable for third pillar;<br>• Officer liable for technical maintenance;<br>• Data protection officer. |
| **Luxembourg** | Yes, cf. 1.3 |
| **Netherlands** | The security role is delegated to the CISlo and daily events can only be effective via the CIS-authorizer. Requests for authorization for the BQT and AFIS are introduced via IM (Information Management) Rotterdam and after granting the request the use of BQT and CIS is possible. Official guidelines are to be improved/ more documented regarding the changing situation. Access to CIS is only possible via the network login name and password and thereupon CIS login name and – password. For CIS the access is granted via B/CICT (Belastingdienst (Tax authorities)/ ICT Centre), IM Rotterdam and the CISlo/ CIS-authorizer. On a daily basis each unit is responsible for its own task. |
| **Poland** | The Ministry of Finance did not prepare the security policy for CIS system (only for AFIS). |
| **Slovakia** | Yes. |
| **Slovenia** | Yes. |
| **Sweden** | New regulations (TFS) regarding the Swedish Customs' processing of data relating to crime fighting activities are being developed in consultation with the Data Inspection Board (Act 2005:787, ordinance 2005:791). |

2.2 Do the security role(s) and responsibilities include the requirement to:
a) implement and act in accordance with the security policy?

| | |
|---|---|
| **Austria** | The role of the security officer also includes the responsibilities as described in the point a |
| **Belgium** | See 2.1 |
| **Czech Republic** | The security measures applied to the CIS are identical with those laid down in the documents as follows:<br>- Security Policy of Customs' Information Systems,<br>- Security System Project of Customs' Information Systems,<br>- Security Standard of Customs' Information Systems,<br>unless provided otherwise in the Service Instruction on Customs Information System (No. 76/2004). |
| **Cyprus** | Yes |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | Yes. |
| **Greece** | Yes. |
| **Hungary** | Yes, the ISR includes the roles and responsibilities as described in point a |
| **Ireland** | Yes. |
| **Italy** | Yes. |
| **Latvia** | The requirements are regulated in IS security policy and instruction of Ministry of Finance Nr.678 (28.july 2004)"Order on how the SRS ensures the access to the EU common data exchange network CCN." |
| **Lithuania** | The assigned officers must implement CIS security policy according to Customs Department Director General order No. 1B-101 of 2006 February 20 article 3.1. |
| **Luxembourg** | Yes. |
| **Netherlands** | Access and authorization integrated in use of network |
| **Poland** | Functions and obligations connected to ensuring the security stand in accordance with the documentation on the operational procedures. All computers connected to the Ministry's of Finance network (including CIS terminals) work under the procedures adopted in the Ministry. Responsibility for taken actions rests upon authorized persons (recently 2 persons). Up to that moment there was no breach of security of data processing conducted by CIS so there are no specific procedures of informing about such breaches or possible dangers in the Ministry. There are some internal procedures applicable. |
| **Slovakia** | Yes. Central Unit for CIS is obliged to protect information, data and documents in the line with legislation in force and approved internal rules of customs administration. |
| **Slovenia** | Yes, since CARS employees are obliged to protect information, data and documents in line with legislation in force and approved CARS standards. |
| **Sweden** | Yes. |

b) protect assets from unauthorized access, disclosure, modification, destruction or interference?

| | |
|---|---|
| **Austria** | The role of the security officer also includes the responsibilities as described in the point b |
| **Belgium** | See 2.1 |
| **Czech Republic** | same as a). |
| **Cyprus** | Yes |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | Yes, the ISR includes the roles and responsibilities as described in point b |
| **Ireland** | Yes. |
| **Italy** | Yes. |
| **Latvia** | The requirements are regulated in IS security policy and instruction of Ministry of Finance Nr.678 (28.july 2004)"Order on how the SRS ensures the access to the EU common data exchange network CCN." |
| **Lithuania** | All CIS users and administrators must fulfill information, equipment and access security procedures according to Customs Department Director General order No. 1B-441 of 2006 June 30. |
| **Luxembourg** | Yes. |
| **Netherlands** | Access and authorization integrated in use of network |
| **Poland** | as a) |
| **Slovakia** | Yes. Information Security Policy (ISP) is introduced and applied on the base of approved internal rules of customs administration. |
| **Slovenia** | Yes. In CARS a System of information security (SIS) and a Information security policy (ISP) are introduced and applied. |
| **Sweden** | Yes. |

c) execute particular security processes or activities?

| | |
|---|---|
| **Austria** | The role of the security officer also includes the responsibilities as described in the point c |
| **Belgium** | See 2.1 |
| **Czech Republic** | same as a). |
| **Cyprus** | Yes |
| **Denmark** | ? ? |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | No. |
| **Hungary** | Yes, the ISR includes the roles and responsibilities as described in point c |
| **Ireland** | Yes. |
| **Italy** | Yes. The security action plan contains all the activities and specific processes in place within the Agency. |
| **Latvia** | The requirements are regulated in IS security policy and instruction of Ministry of Finance Nr.678 (28.july 2004)"Order on how the SRS ensures the access to the EU common data exchange network CCN." |
| **Lithuania** | General Customs information security policy and CIS exploitation policy contains following security features:<br>• Passwords management;<br>• CIS data entrance and validation;<br>• CIS users management;<br>• CIS data legitimacy surveillance. |
| **Luxembourg** | No. |
| **Netherlands** | Access and authorization integrated in use of network |
| **Poland** | as a) |
| **Slovakia** | Yes. The particular security processes or activities are also covered by responsibilities of security officer. |
| **Slovenia** | Yes – security procedures and activities are executed partially by fields of business and with regard to the level of IT support. |
| **Sweden** | Yes. |

d) ensure responsibility is assigned to the individual for actions taken?

| | |
|---|---|
| **Austria** | The role of the security officer also includes the responsibilities as described in the point d |
| **Belgium** | See 2.1 |
| **Czech Republic** | same as a). |
| **Cyprus** | The Department of Customs and Excise ensures that access to CIS is performed by authorised staff only; however audits to the audit logs are not performed by the Department of Customs and Excise but by the Information Technology officer from the Department of Information Technology Services that is assigned for this task. |
| **Denmark** | |
| **Estonia** | Yes |
| **Finland** | Yes. |
| **Greece** | Yes. |
| **Hungary** | Yes, the ISR includes the roles and responsibilities as described in points d |
| **Ireland** | Yes. |
| **Italy** | Yes. |
| **Latvia** | The requirements are regulated in IS security policy and instruction of Ministry of Finance Nr.678 (28.july 2004)"Order on how the SRS ensures the access to the EU common data exchange network CCN." |
| **Lithuania** | Personal responsibility for actions of CIS users and administrators are foreseen by general Customs information security policy, CIS exploitation policy and other Lithuanian legal acts. |
| **Luxembourg** | Yes. |
| **Netherlands** | Access and authorization integrated in use of network |
| **Poland** | as a) |
| **Slovakia** | Yes. |
| **Slovenia** | Yes, but the assigned responsibility depends on the individuals range of activities and information support that individual manages (is assigned to him); ISP imposes operational as well as IT guardianship and horizontal responsibility of the CARS employees and users of IT support; OLAF/CIS provides procedures, functions and with this correlated rights/responsibilities. |
| **Sweden** | Yes, but the employee's manager is entitled to approve. |

e) report security events or potential events or other security risks to the national responsible authority for CIS?

| | |
|---|---|
| **Austria** | The role of the security officer also includes the responsibilities as described in the point e |
| **Belgium** | See 2.1 |
| **Czech Republic** | same as a). |
| **Cyprus** | At the moment not such events have occurred. If such events occur in the future, the Department of Customs and Excise will report it to the Commissioner's Office for the Protection of Personal Data, which is the national authority responsible for the supervision of CIS. |
| **Denmark** | Not relevant. |
| **Estonia** | Yes |
| **Finland** | Yes. |
| **Greece** | No. |
| **Hungary** | Yes, the ISR includes the roles and responsibilities as described in points e |
| **Ireland** | Yes. |
| **Italy** | Yes. Any events or potential risks are periodically reported to the national authority for possible adjustments. |
| **Latvia** | The requirements are regulated in IS security policy and instruction of Ministry of Finance Nr.678 (28.july 2004)"Order on how the SRS ensures the access to the EU common data exchange network CCN." |
| **Lithuania** | General Customs information security policy and Customs Department Director General order No. 1B-417 of 2006 June 10 "On approval of Customs helpdesk order" anticipate security infringements information procedures. |
| **Luxembourg** | Yes. |
| **Netherlands** | Access and authorization integrated in use of network |
| **Poland** | as a) |
| **Slovakia** | Yes. |
| **Slovenia** | Yes in accordance with CIS Manual. At the same time SIS and ISP also regulate the procedures put |

| | |
|---|---|
| | in place for the security events. |
| **Sweden** | Yes. |

## 3. INFORMATION SECURITY AWARENESS, EDUCATION, AND TRAINING.

All employees of the national responsible authority for CIS should have received appropriate awareness training and regular updates in CIS policies and procedures, as relevant for their job function. Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role.

3.1 How has the training proposed in the CIS Manual been applied by the local authorities?

| | |
|---|---|
| **Austria** | On request of the Ministry of Finance the customs offices nominated officers as AFIS-CIS users and sent them to the trainings. The trainings were provided by national trainers educated by OLAF. According to the dependence of the use of the system the trainings were held as two-day or one-day seminars (only border query tool) in special training environments. |
| **Belgium** | The training proposed in the CIS Manual has not been yet applied by the local authorities. |
| **Czech Republic** | In the Czech Republic there are 3 types of training:<br>Training of coordinators – 2-day seminar focused on detailed issues of CIS, including practice in training version of CIS; users' rights are allotted after completing this seminar.<br>Training of registered users – 1-day seminar focused on detailed issues of CIS, including practice in training version of CIS; users' rights are allotted after completing this seminar.<br>Training of unregistered users – half-a-day presentations for selected employees focused on questions and usage possibilities of CIS.<br>Furthermore, training is provided for new employees when necessary. |
| **Cyprus** | As in 1.3. |
| **Denmark** | The employees, who are authorized to use CIS, participate in a course where they learn about the use of CIS and the security policy. |
| **Estonia** | The training session contains Security Policy related information and updates. |
| **Finland** | The security education has been given to all users of CIS. |
| **Greece** | All the users are trained. Training is a pre-requisite for getting access to CIS. |
| **Hungary** | Using and safety measures of CIS is part of the curriculum in the Customs and Finance Guard School of HCFG. If needed the personnel of local organs can have additional seminar-like training. Updated documents in relation to CIS are accessible in the intranet. |
| **Ireland** | All authorized users have been trained to required standard by our Revenue Training Centre in compliance with CIS manual. In addition, refresher training has been provided to all authorized users during July 2006, covering all issues of CIS policies/procedures. |
| **Italy** | Before joining to the CIS, employees are trained by local tutors on the related procedures and liabilities. |
| **Latvia** | All AFIS/CIS authorized users participate in OLAF organized trainings and workshops. |
| **Lithuania** | Until now 3 customs officers were train in OLAF, Brussels, and 2 officers at national level. In the year 2007 Customs Department is planning to start CIS training course for new CIS users. |
| **Luxembourg** | The training proposed in the CIS Manual has been organized according to these guidelines |
| **Netherlands** | One on one education/training. Ongoing. To be executed (further) in 2007. Training takes place in a one on one ore one on two situation by the CIS-authorizer(s). Practice takes place in the network in a special environment. Training will take place in two sessions for each person with in between practice on their own in the special environment. Legislation is explained and several cases are to be evaluated for legislation, appropriate action and other available information. Decisions are made by the CIS-user. Trial-cases are entered under the training-environment and discussed afterwards. After these sessions the CIS-user should be able to enter CIS-cases on their own. Authorization always takes place so the quality of each case is guaranteed |
| **Poland** | Every employee of the national entity responsible for CIS should be properly trained in order to rise conscience and they should be kept updated on the information concerning policies and procedures accordingly to their working post. The training should allow to notice biggest problems concerning security of information and fulfilling their needs. While implementing the CIS system there was conducted a technical training (how to use the system). The training was conducted in the Ministry of Finance and in customs chambers throughout the country. The directors of customs chambers and heads of departments of the Ministry select the participants. After Polish accession to the European Union only one training terminal was left in order to do some additional training. This terminal has been remade into product ional terminal so the training terminal is currently out of use because of the possibilities of security breach. All persons authorized to use CIS system were trained on how to use this system. Instructions concerning operational procedures of CIS have been used for training purposes. During this training the participants got to know about, for instance the safeguards |

| | |
|---|---|
| | connected to the access to the system, principles of organization and exchange of information inside the system, creation, sending and receiving messages by AFIS MAIL, logging on to the CCN gate, making CIS operational, CIS user interface, making the entry, sending the entry to consultation, update, authorization or saving into central data base, searching for data or circulating information. Furthermore, all users of CIS are trained on the safety principles of information systems used in Customs Service. |
| **Slovakia** | On the requirements of CCO guard OLAF training for trainers of application AFIS&CIS and these trainers subsequently provide trainings for other users on national level. |
| **Slovenia** | Six data entry persons (one of them is help-desk) and two authorisers have access to CIS. For all of them, except for one, the training/education was executed by the OLAF. |
| **Sweden** | 8 people took part in the training in Brussels to become teachers. Users in a national level have then been educated by these people. Accounts are only given to those who have taken part in the training. |

## 4. REMOVAL OF ACCESS RIGHTS

The access rights of the users to CIS should be removed upon not usage of the system, termination of their employment, or adjusted upon change.

4.1 Is the national responsible authority for CIS maintaining and updating a users access control diagram?

| | |
|---|---|
| **Austria** | No - such user specific evaluations can only be carried out by OLAF. |
| **Belgium** | The national authority responsible for CIS delegates the user's management to the CIS-LO. The CIS-LO holds a list of the users having access to the CIS. |
| **Czech Republic** | Users of the CIS are filed in an electronic register that is regularly updated or brought up to date according to a situation (new user or deregistration etc.).<br>Within the context of the Board of Customs employees' migration, changes concerning dislocation of employees or termination of their employment are regularly identified. |
| **Cyprus** | A user’s access control diagram is indeed maintained and updated by the Department of Customs and Excise. This Diagram is not only approved by the authorizer but also by the management |
| **Denmark** | When somebody wants to establish a new access to CIS, CISLO sends a form that should be signed be the employee’s employer. This form is kept in a file at CISLO. When the access to CIS should be deleted, the concerned employer notifies CISLO, who deletes the access of the employee. |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | No. |
| **Hungary** | On the Central Law Enforcement Directorate of HCFG there is a list of access rights of the users to CIS. The register contains names, dates of authorization and removal, name of modules to which the user has access. |
| **Ireland** | Yes, responsibility is with national CIS Liaison Officer (CISLO). |
| **Italy** | Yes. A dynamic list of accesses is kept at the Customs Agency’s Headquarters and is maintained and updated by the national responsible authority |
| **Latvia** | The user access control diagram is maintained in accordance with instruction of Ministry of Finance Nr.678 (28.july 2004)”Order on how the SRS ensures the access to the EU common data exchange network CCN.” |
| **Lithuania** | Liaison officer (CISLO) is a main responsible person for users access control. The officer was assigned by Customs Department Director General order No. 1B-101 of 2006 February 20. He is obliged perform constant registration of CIS users and revision of CIS users list. |
| **Luxembourg** | Yes. |
| **Netherlands** | Yes- evaluated once per year |
| **Poland** | The Ministry of Finance is in possession of register of conducted inspections of the CIS system users. Directors of customs chambers are obliged to inform CISLO about any changes concerning CIS users. OLAF must be also informed. |
| **Slovakia** | Yes. CIS user access control diagram is updating by CISLO and the maintaining of the databases is provided by OLAF. |
| **Slovenia** | Yes. The user’s access control diagram is maintained and updated by the CARS CISLO (on request made by head of the department or because of the renewal/changes of human resources). |
| **Sweden** | Yes, since February 2006. The diagram has been sent to Brussels. A new tool, User Registration Tool (URT) is being developed in Brussels. It will enable access administrators in each Member State to constantly receive current data of their users. |

4.2 Does the national responsible authority for CIS control the actual usage of the system and removes user accounts in cases of not usage?

| | |
|---|---|
| **Austria** | Such controls are carried out and user accounts are withdrawn if necessary. The latest control and deletion of inactive user rights was carried out in the end of February 2006. |
| **Belgium** | The national authority and the CIS-LO do not have a monitoring tool which would enable the control of the real use of the system. |
| **Czech Republic** | Yes – such a control is executed on the part of OLAF and the users' accounts are removed after check on national level (on the basis of respective forms). |
| **Cyprus** | Yes, this is done regularly |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | Yes, there is a formalised procedure for this. |
| **Greece** | Yes. |
| **Hungary** | The HCFG can't control the actual usage of the system; this checking can only be carried out by OLAF. |
| **Ireland** | Yes. Accounts maintained and reviewed by CISLO on a three monthly basis. |
| **Italy** | Yes. See above. |
| **Latvia** | Yes, in accordance with instruction of Ministry of Finance Nr.678 (28.july 2004)"Order on how the SRS ensures the access to the EU common data exchange network CCN." |
| **Lithuania** | According to Customs Department Director General order No. 1B-494 of 2005 July 13 all CIS using institutions have immediately to inform CIS liaison officer about their officers' duties change or dismissal. The liaison officer initiates change or rescission of CIS access rights through OLAF helpdesk. |
| **Luxembourg** | YES, an updated list of the users of the Luxembourg customs administration has been sent to OLAF |
| **Netherlands** | Yes - evaluated once per 3 month |
| **Poland** | In the scope of control concerning actual use of the system the Ministry of Finance uses the procedures outlined by OLAF, which sends the queries concerning the use of CIS system periodically. After conducting analysis the information on deactivated user accounts are passed on to the OLAF. |
| **Slovakia** | Yes. The national responsible authority for CIS regularly evaluates national user accounts and also updates these accounts. |
| **Slovenia** | Yes. Because of the small number of the users which are stationed in the same place the control is done through an interview. Until now there has only been change in increasing the level of the authorisation (from data entry person to authoriser). |
| **Sweden** | At present the Swedish Customs does not have access to the central log. When required, data may be requested from Brussels. |

## 5. PHYSICAL AND ENVIRONMENTAL SECURITY

5.1 Are the CIS terminals physically protected from unauthorized access, damage, and interference?

| | |
|---|---|
| **Austria** | As for the CIS terminals, there also exist access restrictions for PCs with national applications in place which are regulated in the data security regulation of the Ministry of Finance. These restrictions are technically individually implemented at the local offices depending on local conditions. |
| **Belgium** | The computers used as terminals CIS are conform to the requirements of the minimum configuration proposed in the OLAF document "Customs information system (CIS) – Security rules" (Bruxelles, 035521 * 05.04.2002, DG/TH D(2002). It concerns desktops (non portable), which are part of the network of the Ministry of Finance. This network is connected to the AFIS network by a link CCN/CSI. An access to Internet is only possible via the Intranet network of the Ministry of Finance, which is secured.<br>The users of the network of the Finance Ministry (including the CIS users) have no administrator rights on their computers. Therefore, they are not able to install themselves software.<br>According to the architecture of the building, the most possible measures are taken to avoid non authorized persons to see the data, even by accident. |
| **Czech Republic** | Physical security of buildings and premises<br>-the rooms where the CIS/AFIS terminals are located are protected by entry controls; the entry is not allowed to unauthorized persons,<br>-an exception is provided for deliverers, security personnel, cleaning stuff, who are allowed entry the |

| | |
|---|---|
| | rooms with the CIS/AFIS terminals accompanied by a CIS user or on the basis of a special authorization,<br>-the rooms with the CIS/AFIS terminals are situated in such a part of building, where an entry control is established (i.e. the entry of unauthorized personnel Is limited),<br>-the rooms with the CIS/AFIS terminals are secured by a code, key or magnetic card.<br>Physical security of the CIS/AFIS terminals<br>-the CIS/AFIS terminals are configured so that there is no access to Internet possible,<br>-duty officers in departments, where the CIS/AFIS terminals are located, shall provide measures to prevent access to CIS data by unauthorized staff, even in an emergency case (e.g. situation of the monitors opposite windows),<br>-while leaving the workplace (the CIS/AFIS terminal) the user is obliged to lock the terminal by an screen saver; the screen saver has to be automatically activated within 5 minutes of inactivity,<br>Localization of printers – to print a document form the CIS is possible only on printers that are located in the same room or near to the CIS/AFIS terminal.<br>Management of CIS<br>1. Competences dividing:<br>o the responsibility for administration of CIS/AFIS on the central level rest upon OLAF, which is among others responsible for client software and central database,<br>o for the communication network CCN/CSI is the General Directory of the Customs of the Czech Republic responsible,<br>o the responsibility for CIS within the Board of Customs of the Czech Republic is in general laid down in the Directive on operating of Customs' Information Systems (No. 2/2002),<br>o for communication network and for establishing user accounts on the national entry (necessary for internal need of the Customs) is a specialized department of the General Directory of Customs responsible,<br>o technical management of CIS/AFIS software falls within responsibility of a respective department; among others this activity includes:<br>? testing and implementation of new versions,<br>? implementation of new versions to end terminals (on the level of the General Directory of Customs),<br>? configuration of local terminals (on the level of the General Directory of Customs),<br>o technical management on the level of Customs Directories and subordinated bodies is provided by specialized department; this activity includes:<br>? implementation of new versions to end terminals,<br>? configuration of local terminals.<br>2. Installation of CIS/AFIS terminals<br>o the first installation is executed by a respective department,<br>o further installations are on the level of Customs Directories and subordinated bodies executed by specialized department on the basis of an appointment of the respective department.<br>3. Servicing of CIS/AFIS<br>o the servicing of CIS/AFIS terminals includes namely:<br>? antivirus definitions actualization,<br>? implementation of security patches to operational system,<br>? diagnostic of technical devices,<br>o the servicing is provided by:<br>? respective department – on the level of the General Directory of Customs,<br>? specialized department - on the level of Customs Directories. |
| **Cyprus** | Yes, according to the action plan and the CIS Manual |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | YES in the Central Site |
| **Hungary** | Yes. The CIS terminals are in the security increased zone. (Note: there are three types of zones: normal, security increased and high security. Different safety measures apply to each zone.) |
| **Ireland** | All CIS terminals are located in secure locations, accessible only by authorised Revenue Personnel. |
| **Italy** | Yes. Instructions on location requirements and physical protection of CIS terminals from unauthorized access, damage and interference are documented. |
| **Latvia** | Requirements are regulated in IS security policy |
| **Lithuania** | Presumably CIS terminals physical protection is sufficient. All CIS terminals are located in locked areas with code access doors. |
| **Luxembourg** | Yes. |
| **Netherlands** | Integrated in network – double login and password. The physical security is arranged according to |

| | |
|---|---|
| | the rules for government buildings. In our case access is only possible through the special pass for accessing the building on the ground floor, subsequently the third floor.<br>CIS-cases are stored in a locked cabinet and the cabinet can only be opened with a key. The use of PC's is only possible for authorized personnel. Servers are not accessible for local personnel, and are stored elsewhere in sealed rooms and/or buildings. |
| **Poland** | CIS terminals are actually protected. Access to CIS system is possible only by 3 computers in the Ministry of Finance. Locked wooden doors protect entrance to the room where these computers are situated. Door to this room is sealed. There is also a note saying, "Entrance to this room is only possible with the consent or in presence of authorized person". Inside the room there is smoke detector. Computers are connected to the separate electro energetic line. Windows of this room are blinded to protect the monitors. Keys to this room are kept in locked and sealed cabinet in the secretariat of Customs-Excise Control and Gambling Control Department. Only two authorized persons have access to these keys. |
| **Slovakia** | Yes. Protect from unauthorized access, damage and interference is regulated by internal provision about regime arrangements. |
| **Slovenia** | Yes. The three (CIS) terminals are physically protected and with passwords. They are only connected with fax, which is also the only installation in the room where the terminals are kept. The terminals are not connected with internet or external environment. |
| **Sweden** | Yes, the physical areas are protected from unauthorized access and each terminal may only be used with a valid smart card. |

5.2. Are the physical areas of the CIS hardware facilities protected by appropriate entry controls to ensure that only authorized personnel are allowed access?

| | |
|---|---|
| **Austria** | To start-up a PC the user has to register with user name and password. The security for computer systems recently has been raised further by a comprehensive system upgrade. The start-up of a PC now only is possible with a locked personal service card. Furthermore the use of AFIS / CIS only is possible with a valid user definition after setup and entry of an individual local and network password.<br>If these required data have been entered repeatedly invalid, access is disabled by the system.<br>After leaving the work place a screensaver will activate. The officer also has to remove his personal service card of the PC to prevent unauthorized access. |
| **Belgium** | According to the architecture of the building, the most possible measures are taken to ensure that only authorized person are allowed access. When there are change regarding hosting, these measures are again taken into account. In case of moving, these measures are taken into consideration. |
| **Czech Republic** | see 5.1. |
| **Cyprus** | Yes, for access to these areas a card and a password is needed and there are also security locks. |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | Yes. Measures in the increased zone for example: register of the authorized personnel; electronic entry-system; visitors are accompanied by officers; use of a PC requires user name and password; access and actions are recorded etc. |
| **Ireland** | Yes. All offices where terminals are located have swipe card or keypad entry to authorised staff. |
| **Italy** | Yes. All terminals are located in rooms where only authorized stuff can access. |
| **Latvia** | Requirements are regulated in IS security policy |
| **Lithuania** | CIS terminals are located in locked areas of customs buildings with code access doors. All customs institutions are using surveillance cameras. |
| **Luxembourg** | YES, protected by User ID and password. |
| **Netherlands** | Integrated in network – double login and password. The physical security is arranged according to the rules for government buildings. In our case access is only possible through the special pass for accessing the building on the ground floor, subsequently the third floor.<br>CIS-cases are stored in a locked cabinet and the cabinet can only be opened with a key. The use of PC's is only possible for authorized personnel. Entry control and use of means of communication is only allowed for authorized personnel |
| **Poland** | Rooms in which the CIS equipment is situated are included in the security system of the Ministry according to the Security Plan agreed with Chief of Municipal Police |
| **Slovakia** | Yes. Entry to the premises is protected with permanent service, in the building is established system |

| | |
|---|---|
| | of control entry. |
| **Slovenia** | Yes, since terminals are located in the room where only authorized personnel can access with special id-registration card and there is also s special security lock. At the same time the premises are properly physical and technical secured with video camera, security guard and permanent control through entry card. Responsibilities and procedures for protection of premises are also regulated by SIS, ISP and CARS house order. |
| **Sweden** | Yes. |

5.3 Has physical security for offices, rooms, and facilities (for CIS users) been designed and applied?

| | |
|---|---|
| **Austria** | For the CIS-users beyond the high national safety standard no further physical measures have been set. The data security regulation of the Ministry of Finance includes regulations with regard to restrictions of access, of use of data systems and in handling of data. |
| **Belgium** | The equipment and the CIS terminals are protected in the same way as the others rooms and equipments of the different departments of the Ministry of Finance. |
| **Czech Republic** | see 5.1 |
| **Cyprus** | Yes |
| **Denmark** | Yes, computers with access to CIS are placed in places, with access control and places where unauthorized persons do not have access. |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | YES in the Central Site. |
| **Hungary** | There aren't additional rules for CIS users, facilities and offices; increased safety measures also apply to CIS users, facilities and offices. |
| **Ireland** | Yes. Offices have swipe card or keypad entry to authorised staff. In general terms it can be stated that all Revenue offices, because of the nature of the confidential material stored, are regarded as secure environments. |
| **Italy** | Partly. A specific document is being designed to improve physical security. |
| **Latvia** | Physical security is provided in every office, room and facility in accordance with contracts concluded with Security company. |
| **Lithuania** | Customs work rooms do not contain specific security measures, except these: locked areas, monitors of CIS terminals are located to the room walls, access to computers and CIS are protected by individual passwords, computers have password protected screensavers and all CIS printing devices are located in the same room as CIS terminals. Access to CIS through Operation Manager is protected by two passwords (Local and Network passwords). |
| **Luxembourg** | YES, offices, rooms, and facilities are under 24h surveillance by a regulated company |
| **Netherlands** | Integrated in network – double login and password. The physical security is arranged according to the rules for government buildings. In our case access is only possible through the special pass for accessing the building on the ground floor, subsequently the third floor.<br>CIS-cases are stored in a locked cabinet and the cabinet can only be opened with a key. The use of PC's is only possible for authorized personnel. Entry control and use of means of communication is only allowed for authorized personnel |
| **Poland** | As it was stated there are no principles concerning the security of rooms, offices, and equipment only for CIS users. Security principles of these facilities results from the security plan. |
| **Slovakia** | Yes. See answers in points 5.1 and 5.2. |
| **Slovenia** | Yes. Physical security for offices and facilities for CIS users has been designed in compliance with CIS procedures and national acts that regulate personal data protection, protection of classified information and protection of data representing tax secrecy. |
| **Sweden** | Yes, the back-office principle is applied, i.e. the terminals are not located in connection with the reception area for visitors. |

## 6. CONTROLS AGAINST MALICIOUS CODE

6.1 Are the computer where the CIS is installed having access to the Internet?

| | |
|---|---|
| **Austria** | Yes - the PCs of the financial administration are multifunctional terminals where besides different standard software applications and Internet access the CIS is installed. The Internet may only be accessed by the Internet-browser made available by the IT department of the Ministry of Finance and according to the IT-safety guideline for the use of Internet for work. For danger prevention virus checking programs, firewall technology, URL filters, spam filters etc. are used systematically and |

| | |
|---|---|
| | ongoing updated. |
| **Belgium** | Yes. Access to Internet is possible but only through the secured Intranet of the Ministry of Finance |
| **Czech Republic** | The CIS/AFIS terminals are configured so that there is no access to Internet possible. CIS software shall not be installed before applying an antivirus program on the computer. The antivirus program is operated in accordance with an internal document – Antivirus Security Principles of Customs' Information Systems. |
| **Cyprus** | Some of the computers have the option to access the Internet but they are not connected to the Internet while using the CIS. |
| **Denmark** | Yes, SKAT applies the internet version of CIS, and therefore it is possible to install CIS on terminals with access to the internet. When gaining access to the internet a proxy server is used. |
| **Estonia** | Yes, through the organization's proxy server. |
| **Finland** | Yes, but access is controlled and according to the safety guidelines. |
| **Greece** | No. |
| **Hungary** | Yes, across the proxy-server with central theme-filtering, with another password, individual authorization and permanent IT supervision |
| **Ireland** | A certain number of computers have internet access, via Revenue secure Intranet facility, but as CIS is accessed via a CITRIX server (proxy), this complies with Security Procedures as set out by OLAF. |
| **Italy** | No. |
| **Latvia** | Yes |
| **Lithuania** | Yes. |
| **Luxembourg** | YES, but controlled by the WEBSENSE! |
| **Netherlands** | Yes, but only for specified url's. B/CICT in Apeldoorn is granting access to a limited amount of URL's and after careful evaluation for authorized personnel. To mention a few: de Beeldkrant, NOS teletekst, Legislation sites. Some of them give access to sites in the intranet (internal network), others give access externally. All these sites are monitored on a regular basis and evaluated by B/CICT according to their procedures. Malicious codes are stopped by adequate software. Access to other mail-addresses is given to a limited group of people and is protected against malicious code by special software. |
| **Poland** | Computers connected to CIS system have no access to the Internet. |
| **Slovakia** | No. |
| **Slovenia** | No. |
| **Sweden** | Yes. |

6.2 Inform if the national responsible authority for CIS has established:

a) a formal policy prohibiting the use of unauthorized software

| | |
|---|---|
| **Austria** | The use of non-authorized software is regulated and prohibited in the guideline for IT safety |
| **Belgium** | The users of the Intranet network of the Ministry of Finance (including the CIS users) have the rights of administrator only when it is necessary to set up software. |
| **Czech Republic** | Security measures for the CIS are identical as for other information systems and are defined in internal documents (Security Policy of Customs' Information Systems, System Protection Project of Customs' Information Systems and Security Standards for Customs' Information Systems). |
| **Cyprus** | Such a policy has been established by the management |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | The annex of ISR contains the list of unauthorized software. The use of non-authorized software is regulated and prohibited in the ISR. Safety controls check whether there is any unauthorized software on the computer. |
| **Ireland** | Revenue has a strict code of practice regarding the use of all computer software. This policy extends to CIS software. |
| **Italy** | Yes. This formal policy applies to all the computers in use in the Agency. |
| **Latvia** | Such prohibition is provided by IS security regulative documents. |
| **Lithuania** | Yes, approved by order 1B-441 of 30 June 2006 of Director General of Customs Department. |
| **Luxembourg** | YES, covered by the Central IT behaviour guidelines of Luxembourg |
| **Netherlands** | Yes. not possible only by IM Rotterdam or B/CICT Apeldoorn. Any use of software without the interference and approval of B/CICT or IM Rotterdam is not possible. To obtain permission for the use of 'own' software you have to have permission from several authorised people and after following testing procedures. Such procedures can take up to one year. Standard answer however of B/CICT is that no permission is given. |

| | |
|---|---|
| **Poland** | Using illegal programming is strictly prohibited in Ministry of Finance. Users with no proper authorization don’t have any possibility to install software on the computers connected to the system. It is also impossible to install software from outside network. All CIS computers have the anti-virus software called Norton Antivirus installed updated on the day to day basis. |
| **Slovakia** | Yes. The unauthorized software is not used in Slovak Customs administration and using of this software types is also strictly prohibited by internal rules of IT security. |
| **Slovenia** | Yes. Software installation is possible by the personnel of sector for informatics that has an administrator rights at single terminal |
| **Sweden** | Yes. |

b) a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken;

| | |
|---|---|
| **Austria** | The handling of files and software from external sources is regulated in the guideline for IT safety. Incoming e-mails and attachments are automatically checked by the system. |
| **Belgium** | Such a policy has not been established by the national responsible authority for CIS. |
| **Czech Republic** | see above. |
| **Cyprus** | A circular has been issued by the management with measures against those risks **. |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | On computers of the HCFG there are ongoing updated virus checking programs, central firewall technology and several filters (spam, URL, e-mail etc.). |
| **Ireland** | As above. |
| **Italy** | Yes. See above. |
| **Latvia** | There are Prohibitions of usage of IS recourses within authorized access assigned for job responsibilities. It is established in IS security regulative documents. |
| **Lithuania** | Yes, approved by order 1B-441 of 30 June 2006 of Director General of Customs Department. |
| **Luxembourg** | Yes. |
| **Netherlands** | The same as a) |
| **Poland** | Yes |
| **Slovakia** | Yes. Obtaining of files from external sources are also one of the important part of IT security rules. |
| **Slovenia** | Yes because of disabled access. |
| **Sweden** | Yes. |

c) installation and regular update of malicious code detection on the CIS computers

| | |
|---|---|
| **Austria** | The anti virus programs are centrally ongoing updated and the up-to-date version is installed automatically. Furthermore a virus check of the most important system files is carried out automatically during every start-up of the PC. |
| **Belgium** | The installation and regular update is done in a centralized way by the ICT department of the Ministry of Finance |
| **Czech Republic** | see above |
| **Cyprus** | Yes, antivirus software that is daily updated |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | In accordance with the central default of the CIS-program the access is blocked automatically if a wrong user name or password is entered 10 times. |
| **Ireland** | As above. |
| **Italy** | Yes. |
| **Latvia** | On computers are installed antivirus software that are regularly updated. |
| **Lithuania** | Yes, approved by order 1B-441 of 30 June 2006 of Director General of Customs Department. |
| **Luxembourg** | Yes. |
| **Netherlands** | The same as a) |
| **Poland** | Yes |
| **Slovakia** | Antivirus program is regular updated. |

| | |
|---|---|
| **Slovenia** | No, since this is in the competence of the manager of the application (OLAF). |
| **Sweden** | Yes. |

## 7. MONITORING

The usage of the CIS should be monitored in a national level.
7.1 Are audit logs recording user activities been produced and kept for an agreed period to assist in access control monitoring?

| | |
|---|---|
| **Austria** | On national level it is technically impossible to produce audit logs recording user activities. Only OLAF is able to do this. |
| **Belgium** | Currently, the records of the user's activities are nor produced or kept.<br>As already mentioned on point 4.2, nor the national authority or the CIS-LO do not have a monitoring tool which would enable the control of the real use of the system |
| **Czech Republic** | Yes – logs concerning users’ activity are created and kept in accordance with an internal document (Security Policy of Customs’ Information Systems). |
| **Cyprus** | Yes, audit logs are being produced by the system |
| **Denmark** | No, SKAT is not – in the present version – capable of making log files from CIS. |
| **Estonia** | Yes, CIS database logs are located on the server side, which is located in Brussels. The workstation authentication and user security/audit logs are located in the domain controller logs. |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | In accordance with OLAF, Manual enter or inquiry of data are recorded by OLAF. On national level it is technically impossible to produce audit logs recording user activities, only OLAF is able to do this. |
| **Ireland** | No. We are unaware of any such facility at national level. We are aware that such a facility exists at European level and is being monitored by the Commission. |
| **Italy** | Partly. An initiative to raise the awareness of the responsible managers at a local level has been actuated. |
| **Latvia** | This function is provided by OLAF in accordance with information in OLAF manual. |
| **Lithuania** | At the current time Customs does not produce or keep audit logs with CCN user activities in the system. |
| **Luxembourg** | A new system will be implemented in 2007. |
| **Netherlands** | No yearly, until now via Brussels. Monitoring on a national level is not effective yet, mainly because of the restricted use of CIS. National monitoring will be effective as more personnel is authorized and will take place once per 3 months. Data will be kept for one year. |
| **Poland** | The controlling entries registering actions taken by users like logging to the computer, running applications, logging to the CCN gate (equipment allowing tele transmission between Poland and Brussels) are kept in system logs. Information is kept locally and includes actions taken by users like downloading or mailing data. Information is also kept on paper as letters concerning specific case. In the Ministry of Finance there are no technical possibilities to keep these registers in the CIS central database. OLAF office should supervise such actions. Transmission of data between the CIS end user and central database is coded with the use of 3 DES algorithm. |
| **Slovakia** | No. Only OLAF is responsible for this activity. |
| **Slovenia** | No. The supervision is executed by personal passwords. |
| **Sweden** | The audit logs record who has used the system and for how long. Apart from that there are central logs at OLAF. |

7.2 Is a procedure developed on the audit policy?

| | |
|---|---|
| **Austria** | There is an annual audit planning in the Ministry of Finance for the tax and customs administration. An audit of the CIS is envisaged for next year. |
| **Belgium** | No, there is no formal procedure |
| **Czech Republic** | Yes – audit rules are defined in an internal document (Security Policy of Customs’ Information Systems). |
| **Cyprus** | No, only the information Technology Officer has access to the audit logs and there is no formal policy for the auditing of the logs. |
| **Denmark** | No. A procedure will be developed when it becomes possible for CISLO to make its own log files. |
| **Estonia** | Yes |
| **Finland** | At the moment the audits case-specific analysis are made. The procedure for audit policy is under preparation. |

| | |
|---|---|
| **Greece** | No. |
| **Hungary** | Defects or problems exposed by safety control are analysed and rectification or solution thereof are checked within a given time. |
| **Ireland** | As above. |
| **Italy** | Partly. An operating manual is being drawn up in compliance with the audit policies for systematization. |
| **Latvia** | This function is provided by OLAF in accordance with information in OLAF manual. |
| **Lithuania** | Customs does not form or obtain CIS user audit currently, because of the technical obstacles. |
| **Luxembourg** | Cf. 7.1 |
| **Netherlands** | Yes via Brussels |
| **Poland** | There is no procedure concerning controlling policy. |
| **Slovakia** | Yes. |
| **Slovenia** | Yes. All data or information transmitted from the CARS filing systems must be in accordance with CARS internal rules recorded into the register of transmitted information. |
| **Sweden** | No follow-up. There is no procedure for this. This is expected to be included in the new regulations. |

## 8. ACCESS CONTROL POLICY

8.1 Is there an access control policy established, documented, and reviewed based on the CIS manual?

| | |
|---|---|
| **Austria** | User accounts are assigned by the Ministry of Finance only for those organization units which are considered as users of the CIS (antifraud service in the central tax and customs administration, customs investigation service, risk information and analysis unit, mobile control units, information and communication centres). The users are nominated by the departments and receive their user definition after passing the AFIS-CIS training. As soon as OLAF implements the requested definitions in the system and after the definitions have also been implemented in the CCN gateway on national level the user may have access to the CIS.<br>These steps are documented in the corresponding file records. User accounts could also be deprived if necessary. |
| **Belgium** | No, there is no formal procedure |
| **Czech Republic** | This problematic is laid down in the Service Instruction on Customs Information System (No. 76/2004), which was adopted on the basis of the CIS manual. Access controls are executed in accordance with an internal document (Security Policy of Customs' Information Systems). |
| **Cyprus** | A list of users is maintained, each user has his own I.D and password, and each user has specific rights but there is no separate written policy on this. |
| **Denmark** | Yes, an access control policy as described in the CIS manual has been established. |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes, only trained customs officers have access to CIS.. |
| **Hungary** | Yes, there is a regulation by the General Commander of the HCFG based on the CIS Manual about CIS user rights and work flow. |
| **Ireland** | All access is controlled centrally by CISLO by means of registered user. All registered users are documented, and periodically reviewed by CISLO. |
| **Italy** | Yes. There is a policy for access control adjusted to the updates of the CIS manual and to local analysis. |
| **Latvia** | Yes |
| **Lithuania** | Yes, Customs has an access control policy approved by order 1B-494 of 13 July 2005 of Director General of Customs Department. |
| **Luxembourg** | YES, the access control policy will be reviewed in 2007 |
| **Netherlands** | Yes |
| **Poland** | Access control policy concerning specific rights in CIS depends on the preparation of motion by the user, which should be verified by Customs -Excise Control and Gambling Control Department and by proper body of the OLAF relating to rights under motion. Actual access to CIS terminals is registered in written form (there are plans of protecting the venues with the electronic access control system). Access control policy is inspected on the grounds of Instruction of CIS procedures and the principles of control of access rights of every individual user are given in the access control policy. |
| **Slovakia** | Yes. |
| **Slovenia** | Yes. |
| **Sweden** | Yes. |

8.2 If yes, are access control rules and rights for each user or group of users clearly stated in this access control policy?

| | |
|---|---|
| **Austria** | The user rights and definitions correspond with the tasks of the defined users and are documented in the standardized application to OLAF for the definition of the user rights. |
| **Belgium** | - |
| **Czech Republic** | The same as above |
| **Cyprus** | - |
| **Denmark** | Yes |
| **Estonia** | The Access Control Policy that exists does not state access control rules and rights for each user or group of users. This however is stated in a different document, Policy of the use of Information Systems of Estonian Tax and Customs Board which is in accordance with the CIS Manual. |
| **Finland** | The uses rights correspond wit the tasks of the users. |
| **Greece** | Yes. |
| **Hungary** | The above mentioned updated regulation is accessible in the intranet. |
| **Ireland** | Each registered user has individual rights, as determined by CISLO. |
| **Italy** | Yes. |
| **Latvia** | Yes |
| **Lithuania** | Yes. |
| **Luxembourg** | Each user or group of users have defined their access rights by the local and central access policy of the Luxembourg customs administration. |
| **Netherlands** | Yes |
| **Poland** | Yes |
| **Slovakia** | Yes, they are regulated by internal rule. |
| **Slovenia** | Yes. |
| **Sweden** | Yes. |

## 9. USER ACCESS MANAGEMENT

9.1. Are any formal procedures to control the allocation of access rights to the CIS?

| | |
|---|---|
| **Austria** | User accounts are assigned by the Ministry of Finance only for those organization units which are considered as users of the CIS (antifraud service in the central tax and customs administration, customs investigation service, risk information and analysis unit, mobile control units, information and communication centres). The users are nominated by the departments and receive their user definition after passing the AFIS-CIS training. As soon as OLAF implements the requested definitions in the system and after the definitions have also been implemented in the CCN gateway on national level the user may have access to the CIS.<br>The IT department of the Ministry of Finance informs the defined users that the definition has been implemented and provides the software (CD-ROM) with the entry password and further information about the handling of passwords. |
| **Belgium** | No, there are no formal procedures |
| **Czech Republic** | Establishment of user account<br>-a registered user account is established on the basis of a request, signed by respective officers only. This request is forwarded to a responsible department, which provides for establishment of user account by respective organ of European Commission. Subsequently the responsible department informs the user that an account was established and forwards him ID and password to the CIS,<br>-the responsible department forwards ID and password to CCN portal, which are provided by controller of the national entry,<br>-ID and password are sent to the user separately (e.g. in a different parcel or by different means).<br>CIS/AFIS terminal obtaining<br>-due to security as well as technical reasons is number of CIS/AFIS terminals and number of registered users limited,<br>-in case a customs authority requires new or another one CIS/AFIS terminal or intents to relocate a terminal to different room or building is before doing so obliged to sent a request to the responsible department where specifies the reason of the request and expected contributions, frequency of usage and results. Furthermore, customs authority are usually obliged to enclose a detailed plan of the room (out of which is the placement of the new or relocated terminal visible) and documents concerning all security measures,<br>-the responsible department is entitled to deny the request on new terminal or on relocation of a terminal due to security reasons. |

| | |
|---|---|
| **Cyprus** | Formal procedures have been adopted by the management |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | The HCFG adopted the form and process of access rights elaborated by OLAF. |
| **Ireland** | Yes, via CISLO. |
| **Italy** | Yes. |
| **Latvia** | Yes, allocation of access rights to the CIS is accomplished in accordance with instruction of Ministry of Finance Nr.678 (28.july 2004)"Order on how the SRS ensures the access to the EU common data exchange network CCN." |
| **Lithuania** | Yes, this issue regulated by order 1B-494 of 13 July 2005 approved by Director General of Customs Department. |
| **Luxembourg** | YES, access rights are formally allocated by the directorate of the Luxembourg customs administration |
| **Netherlands** | Yes by / via IM Rotterdam or B/CICT Apeldoorn. Comparison of data from IM Rotterdam with available data from 'Brussels' takes place once a year. |
| **Poland** | Security measures taken for CIS system are among others: authorization process, 3 steps of logging to the AFIS/CIS system. Individual login and password is used. Transmission of data is realized in separate information network of the Ministry of Finance (WAN network). Control of giving authorization to access CIS is conducted under specific procedures but OLAF is responsible for the configuration of users. Indicated procedures are related to all levels of user's access from the registration of new users to final erasure. |
| **Slovakia** | Yes. Internal rule of CCO about operation of CIS is valid. |
| **Slovenia** | Yes. |
| **Sweden** | Yes. |

9.2. The procedures cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to the CIS?

| | |
|---|---|
| **Austria** | Yes - all stages of a cycle of user access are covered by the standardized OLAF-application form. |
| **Belgium** | - |
| **Czech Republic** | see above. |
| **Cyprus** | Yes. The management approves user access. OLAF is informed in writing in case of a de-registration of a user. |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | Yes |
| **Ireland** | Yes, via CISLO. |
| **Italy** | Yes. |
| **Latvia** | Yes, procedures cover all stages in the life-cycle of user access. It is accomplished in accordance with instruction of Ministry of Finance Nr.678 (28.july 2004) "Order on how the SRS ensures the access to the EU common data exchange network CCN |
| **Lithuania** | The order of Customs Department Director General No. 1B-494 of 2005 July 13 foresees requirements for CIS users registration and de-registration. Officer may be registered as CIS user by implementing following requirements: permission to work with information "EU Restricted" and application with provision of personal data plus services duties description for CIS access. Responsible person for registration of CIS users is CIS liaison officer (CISLO). |
| **Luxembourg** | Cf. 4.1, there is no written procedure for the moment |
| **Netherlands** | Same as above. |
| **Poland** | Yes |
| **Slovakia** | Yes. CCO has approved internal rule about operation of CIS. This rule involve registration form for<br>CIS users<br>and about registration or de - registration decide CISLO. |
| **Slovenia** | Yes. |
| **Sweden** | The user accounts are currently being reviewed and a list of accounts that are to be removed has been sent to Brussels. See 4.1 above. |

## 10. User registration

10.1 Is a formal user registration and de-registration procedure in place for granting and revoking access to the CIS?

| | |
|---|---|
| **Austria** | At present a formal written description of this procedure does not exist, but a standard-workflow has been developed including all involved organisation units (Ministry of Finance, customs offices, users, IT department of the Ministry of Finance, OLAF). |
| **Belgium** | The user registration en de-registration are proposed by the hierarchy of the services concerned to the CISLO that communicates the request to OLAF. No formal procedure is established. However, the relevance of the request is evaluated by the hierarchy. |
| **Czech Republic** | -dispose of an authorization for access to the CIS given by his superior,<br>-absolve a specialized training focused on CIS problematic,<br>-be familiar with all security measures and confirm that by his signature. |
| **Cyprus** | Yes |
| **Denmark** | Yes, look under point 4.1. |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | Yes, see also 9.1. answer. |
| **Ireland** | Yes, via CISLO. |
| **Italy** | Yes. Formal procedures for granting and revoking access are in place. |
| **Latvia** | Yes, CIS user registration and de-registration is accomplished in accordance with instruction of Ministry of Finance Nr.678 (28.july 2004)"Order on how the SRS ensures the access to the EU common data exchange network CCN." |
| **Lithuania** | Yes, this issue regulated by order 1B-494 of 13 July 2005 approved by Director General of Customs Department. |
| **Luxembourg** | Cf. 9 |
| **Netherlands** | Yes by / via IM Rotterdam or B/CICT Apeldoorn. Comparison of data from IM Rotterdam with available data from 'Brussels' takes place once a year. |
| **Poland** | Functioning procedure of registering and erasing users used to grant access to the CIS system results from the rights and obligations of CISLO as well as from the "instruction of operational procedures of CIS". Tasks of CISLO include cooperation between customs chambers and OLAF in the scope of registering, erasing or modifying user accounts in CIS and the AFIS MAIL module. Directors of the customs chambers pass the application forms of new users to those systems (or changes made to the entries). After verification the forms are sent back to OLAF by AFIS MAIL. OLAF sends confirmations the same way. Next CISLO directs a letter to the IT Department of the Ministry of Finance requesting to grant network password to the CCN/CSI gate. After acquiring password CISLO receives the protocol on giving accounts and passwords of users together with protected passwords. Passwords are put into envelopes and together with guidelines concerning local passwords are sent to the directors of customs chambers. Withdrawing of rights is made the same way upon the motion of the director of customs chamber. |
| **Slovakia** | Yes. Passed internal rule of CCO about application of CIS descript granting and revoking access to the CIS. |
| **Slovenia** | Yes. |
| **Sweden** | Yes. |

## 11. User password management

11.1 Is the allocation of passwords controlled through a formal management process?

| | |
|---|---|
| **Austria** | Yes-the user assigns an individual password after the first log in. The access is blocked automatically if a wrong password is entered repeatedly. A password-reset occurs only after a written request of the user. In order to guarantee a complete periodical change of the passwords according to certain safety criteria like for some national Austrian IT applications it would be useful to develop and implement such a routine at OLAF level. |
| **Belgium** | No, there is no formal procedure |
| **Czech Republic** | Users of the CIS are filed in an electronic register that is regularly updated or brought up to date according to a situation (new user or deregistration etc.).<br>Within the context of the Board of Customs employees' migration, changes concerning dislocation of |

| | |
|---|---|
| | employees or termination of their employment are regularly identified. |
| **Cyprus** | The allocation of passwords is controlled by a formal management process of the Department of Information Technology Services |
| **Denmark** | Yes |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | User changes the centrally adjusted password to individual password upon entering the system for the first time. |
| **Ireland** | Yes via ITCeB (Revenue’s computer admin. area) |
| **Italy** | Partly, The process is implemented, although at present no formal management process is in place. |
| **Latvia** | Yes, CIS user rights including allocation of passwords are accomplished in accordance with instruction of Ministry of Finance Nr.678 (28.july 2004)”Order on how the SRS ensures the access to the EU common data exchange network CCN.” |
| **Lithuania** | Yes, this issue is regulated by order 1B-494 of 13 July 2005 approved by Director General of Customs Department. |
| **Luxembourg** | YES, the passwords policy applies to all systems, in accordance to the Central IT behaviour guidelines. |
| **Netherlands** | Yes by / via IM Rotterdam or B/CICT Apeldoorn |
| **Poland** | The passwords are given out on the grounds of the guidelines included in the “Instruction of operational procedures of CIS” but to increase the level of security the number of digits in the password was enlarged from 6 to 8 digits. Furthermore, the procedures of managing passwords were outlined by the IT Department of the Ministry of Finance. |
| **Slovakia** | Names and passwords are created on the national gate CCN/CSI and then they are forwarded through CISLO to CIS users. |
| **Slovenia** | User receives from the CARS CISLO his username and password that has to be changed at the first use. |
| **Sweden** | Yes. |

## 12. REVIEW OF USER ACCESS RIGHTS

12.1 Does the responsible authority for CIS should review users’ access rights to CIS at regular intervals (e.g. a period of 6 months, and after any changes, such as promotion, demotion, or termination of employment) using a formal process?

| | |
|---|---|
| **Austria** | The user rights are reviewed periodically - usually with every software update (on average one per quarter). |
| **Belgium** | The user access rights are reviewed at the time of some events like promotion, transfer, reorganization of the service,…There is no review at regular intervals. |
| **Czech Republic** | Users of the CIS are filed in an electronic register that is regularly updated or brought up to date according to a situation (new user or deregistration etc.).<br>Within the context of the Board of Customs employees' migration, changes concerning dislocation of employees or termination of their employment are regularly identified. |
| **Cyprus** | Yes |
| **Denmark** | Yes, this is reviewed at regular intervals. |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | The allocation of access rights to the CIS is checked randomly. Leaving or suspended officer’s access rights are cancelled in one workday |
| **Ireland** | The majority of users have same standard rights. Where changes in staff arise, CISLO will complete a deletion form and notify the Commission. |
| **Italy** | Yes. The users’ access rights list is reviewed and updated after changes. |
| **Latvia** | Yes |
| **Lithuania** | According to order of Customs Department Director General No. 1B-494 of 2005 July 13 all institutions, which have access to CIS and are using it, have immediately to inform CIS liaison officer about their officers’ duties changes or dismissal. The CIS liaison officer initiates change or rescission of CIS access rights through OLAF helpdesk. |
| **Luxembourg** | Cf. 4.1 |
| **Netherlands** | Yes. Comparison of own data, data from IM Rotterdam with available data from ‘Brussels’ takes place once a year. |
| **Poland** | Problems concerning the verification of user’s access to CIS are realized up to date according to the |

| | |
|---|---|
| | procedures. The day to day control eliminates the need for conducting controls periodically. |
| **Slovakia** | Yes. User rights are reviewed at average 2 times in a period of 6 months. |
| **Slovenia** | Because the users are small in number and stationed in the same place review of the users access rights is done simultaneously and not at regular intervals. |
| **Sweden** | Yes. |

## 13. PASSWORD USE

13.1 Have the users been trained to follow good security practices in the selection and use of passwords?

| | |
|---|---|
| **Austria** | The defined users are informed in the course of the training about the good choice of a safe password during their first access. Furthermore for national applications a periodical password change following pre-defined safety criteria is compulsory – a similar solution is recommended for CIS. |
| **Belgium** | The users are verbally informed of the security practices at the time they are informed of their registration as user. |
| **Czech Republic** | Measures relevant to password<br>- the user is obliged to respect following principles:<br>o change password at the first log-on to the CIS,<br>o choose such a password that is not easily guessed; it is prohibited to use names, personal data, addresses, dates of birth etc.,<br>o change the password every third month,<br>o don’t share the password, including his superiors,<br>o in case of any indication of compromise change the password immediately,<br>o don’t use identical password for different systems,<br>o choose password with minimum length of 7 and maximum of 8 signs,<br>o don’t share individual passwords,<br>o don’t use identical password for business and non-business purposes,<br>- after 10 unsuccessful attempts for log-on to the system is the user account automatically blocked; restoring of the account is possible only with assistance of the responsible department.<br>Password policy for the CIS is defined in an internal act (Directive on operating of Customs’ Information Systems No. 2/2002). |
| **Cyprus** | Yes |
| **Denmark** | Yes, in connection with courses, seminars etc. the users have been informed about god security practices in the selection of password. |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | |
| **Hungary** | Yes. See also 1.4. answer. |
| **Ireland** | Yes, during training process. Also highlighted in Revenue’s IT Code of Practice. |
| **Italy** | Yes. The initial training provides also policies for selecting and using passwords. |
| **Latvia** | Yes, principles and practice of password usage are documented in IS security regulative documents. |
| **Lithuania** | Yes, by initiative of Interior ministry of Republic of Lithuania, 10 customs officers were train. Also Customs Department is planning to start distant security training for all officers and employees of it in the beginning of 2007. |
| **Luxembourg** | Cf. Central IT behaviour guidelines |
| **Netherlands** | Yes. Normal Procedure. Each colleague at the CIC is made aware of the protocols about privacy and integrity as a customs officer by the Ministry of Finance and in particular the CIC. |
| **Poland** | All users of CIS system were trained on the scope of good practice, choice and use of passwords, especially: keeping passwords confidential, avert saving passwords; changing passwords every time when the system or password is endangered; choosing proper passwords with adequate level of length and complexness; frequency of password changes. There is a policy of password changing concerning CIS passwords on the national level.<br>For gaining access to data stored in the local database of the CIS system (on specific computer) it is required to log into the operational system of this computer (Windows 2000 Pro). This requires giving proper identification and 8 digit password. Access to the central database is in addition protected by two loggings. All loggings require entering of the identification and password. Passwords shall consist of no less then 8 digits. |
| **Slovakia** | Creating of passwords is fully in competence of national gate administrator CCN/CSI, which randomly generates passwords and the user has the obligation to change his password always after |

| | |
|---|---|
| | first access. |
| **Slovenia** | All users have been acquainted with the security practice at the OLAF's trainings and through OLAF's Manual that they have received. At the same time the security practice in the selection and use of passwords has already been introduced in some of the CARS information systems and applications (e.g. in certain time frame system automatically requests password to be changed) and standards. |
| **Sweden** | Yes. |

13.2 Were the users advised to:

a) keep passwords confidential;

b) avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;

c) change passwords whenever there is any indication of possible system or password compromise;

d) select quality passwords with sufficient minimum length which are:

1) easy to remember;

2) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;

3) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);

4) free of consecutive identical, all-numeric or all-alphabetic characters;

e) change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;

f) change temporary passwords at the first log-on;

g) not include passwords in any automated log-on process, e.g. stored in a macro or function key;

h) not share individual user passwords;

i) not use the same password for business and non-business purposes.

| | |
|---|---|
| **Austria** | Yes |
| **Belgium** | see 13.1 |
| **Czech Republic** | see 13.1 |
| **Cyprus** | Yes |
| **Denmark** | Yes, compare point 13.1. |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | "No" for a,b,c,d2,d3,d4, e, h, i. "Yes" for the rest |
| **Hungary** | Yes, the above mentioned rules are in the ISR and they are emphasized in trainings. |
| **Ireland** | Yes. |
| **Italy** | Yes. See the initial training above. |
| **Latvia** | Password usage is described in IS security regulative documents. |
| **Lithuania** | Article 7 of the order of Customs Department Director General No. 1B-69 of 2006 January 26 foresees the requirements for CIS passwords. All CIS user must familiarize and obligate to act accordingly to CIS exploitation policy documents and CIS Operating Procedures Manual.<br>a yes, b no, c yes, d) 1) No, 2) No 3) No. 4) No. e) No. f) No. g) No. h) Yes. i) Yes. |
| **Luxembourg** | Yes. |
| **Netherlands** | Yes. Normal Procedure. Each colleague at the CIC is made aware of the protocols about privacy and integrity as a customs officer by the Ministry of Finance and in particular the CIC. |
| **Poland** | Yes |
| **Slovakia** | This issue was in detail analyzed by upon mentioned answers of the questions. |
| **Slovenia** | All users have been acquainted with the security practice at the OLAF's trainings and through OLAF's Manual that they have received. At the same time the security practice in the selection and use of passwords has already been introduced in some of the CARS information systems and applications (e.g. in certain time frame system automatically requests password to be changed). |
| **Sweden** | Yes. |

13.3 Is there a password policy applied for CIS in a national level?

| | |
|---|---|
| **Austria** | Yes |
| **Belgium** | No. |
| **Czech** | see 13.1 |

| | |
|---|---|
| **Republic** | |
| **Cyprus** | So far only the Department of Customs and Excise has access to the CIS. |
| **Denmark** | Yes, compare point 13.1. |
| **Estonia** | Yes |
| **Finland** | Yes |
| **Greece** | Yes. |
| **Hungary** | The rules of password use pay regard to the CIS Manual and apply to every systems of HCFG. |
| **Ireland** | Yes, included in Revenue's overall I.T. policy. |
| **Italy** | Yes. Password policies for CIS are the same password policies adopted by the Agency. |
| **Latvia** | Password policy of State Revenue Service is included in IS security regulative documents. |
| **Lithuania** | Yes, the CIS password policy on a national level is applied by order of Customs Department Director General No. 1B-69 of January 26, 2006. |
| **Luxembourg** | Yes, but more strict security controls will be applied after the implementation of the new version of CIS. |
| **Netherlands** | Yes. Normal Procedure. Each colleague at the CIC is made aware of the protocols about privacy and integrity as a customs officer by the Ministry of Finance and in particular the CIC. |
| **Poland** | Yes |
| **Slovakia** | Yes. Password policy is regulated generally. |
| **Slovenia** | All users have been acquainted with the security practice at the OLAF's trainings and through OLAF's Manual that they have received. At the same time the security practice in the selection and use of passwords has already been introduced in some of the CARS information systems and applications (e.g. in certain time frame system automatically requests password to be changed). |
| **Sweden** | Yes. |