ORIGINATOR:	ISSUE DATE:	VERSION:
ATOS ORIGIN	13-Feb-2006	EN3.00

TAXATION AND CUSTOMS UNION DG

CCN/CSI Project

SUBJECT:

CCN/CSI GENERAL SECURITY POLICY

CCN-CSEC-POL

FRAMEWORK CONTRACT TAXUD/00/C063
SPECIFIC CONTRACT 18

DOCUMENT HISTORY

Edi.	Rev.	Date	Description	Action(*)	Paragraphs
0	00	10-Feb-1998	Creation	I	All
1	00	12-May-1998	Minor modifications proposed by the GB administration.	R	8.5, 9.3
2	00	18-Aug-2003	Minor modifications, taking into account the evolution of the CCN/CSI infrastructure	R	All
2	01	30-May-2005	Major rewriting	I, R	All
2	10	03-Jun-2005	Official version sent for review		None
2	11	3-Feb-2006	Taking into account Response_to_DRF_RFA147_CCN-CSEC-POL-EN2.10V2.doc	I, R	All
2	12	3-Feb-2006	Internal Quality Review	I, R	All
2	20	3-Feb-2006	Official Version Delivered for Review		None
2	21	9-Feb-2006	Taking into account Conference Call 09-Feb-2006	I, R	§3.2, §5.1.1, §5.1.3, §6.2, p1
2	22	10-Feb-2006	Internal Quality Review	I, R	All
2	30	10-Feb-2006	Official Version Delivered for Review		None
3	00	13-Feb-2006	Official Version Delivered for Acceptance		None

(*) Action: I=Insert R=Replace

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 PURPOSE OF THIS DOCUMENT

This document defines the General Security Policy for the CCN/CSI infrastructure.

More than just depicting general security principles, it provides a security framework for CCN/CSI, including:

- The definition of Security Objectives for CCN/CSI (What);
- The definition of the Security Domain (Where);
- The definition of ownership and responsibilities (Who);
- The description of the CCN/CSI Information Security Management System (How)
  - Introduction to the principles of Assets classification; Risk Assessment, Risk Mitigation, Monitoring, Auditing, Reviewing)
  - An introduction the Matrix of Security Measures (extensive "database" of Security Measures used to achieve the Risk Mitigation);
- The CCN/CSI security documentation baseline (i.e. list of references to documents focusing on CCN/CSI security);
- A process flow for achieving compliance with the CCN/CSI Security Policy;
- The CCN/CSI Security Compliance Checklist.

The procedures concerning the management of Information Security within the CCN/CSI community are outlined in this document.

Practical procedures in support of CCN/CSI, including security components, will be introduced here but detailed in the CCN/CSI Practical Security Guidelines [RD13]

All CCN/CSI security-related documents are listed in section 2.2.

1.2 STRUCTURE OF THE DOCUMENT

The document is made of the following sections:

Section 1 Introduction

This section describes the purpose of this document, its field of application and a description of its structure.

Section 2 Documents

This section gives pointers to applicable and reference documents used as an input to this document.

Section 3 Glossary

This section provides a glossary of terms and acronyms used in this document.

Section 4 CCN/CSI Information Security Objectives (What)

This section describes the CCN/CSI Information Security Objectives, defining what has to be achieved in order to satisfy the CCN/CSI and DG TAXUD security expectations.

Section 5 Security Domain (Where)

This section describes what are the components and the borders of the Security Domain. The jurisdiction of this Security Policy is defined in this chapter.

Section 6 Parties and Responsibilities (Who)

This section describes what are the parties and what is the split of responsibilities enforcing the Security Objectives upon the Security Domain.

Section 7 CCN/CSI Information Security Management System (How)

This section describes the new Information Security Management System (a tailor made mix of the ISO/IEC 17799 standard and the Information Security Forum model).

In a nutshell, this ISMS is the strategic model that drives the "Risk Assessment – Risk Mitigation – Monitoring, Auditing & Review" process chain in order to achieve the Security Objectives.

Appendix A CCN/CSI Security Compliance Process

A description of the Security Compliance process. The various sites and components of the CCN/CSI must adhere to the CCN/CSI Security Policy and enforce the appropriate Security Measures to achieve the required security level.

1.3 FIELD OF APPLICATION

The present document is applicable to the operational usage of the CCN/CSI infrastructure by the National Administrations, the European Commission (TAXUD, OLAF et DATA CENTRE), and the CCN/TC.

1.4 INTENDED AUDIENCE

The intended readership for this document includes:

- All the parties and responsibles defined in the section 6;
- Those responsible for designing and implementing CCN/CSI including its security features;
- Those responsible for the definition of the functional and technical specification of CCN/CSI;
- Those responsible for designing, implementing, and managing DG TAXUD applications;
- Any other authorised body concerned with the CCN/CSI including, but not limited to the CCN/CSI Joint Committee, Steering Committee, DG TAXUD and OLAF.

Readers are expected to be familiar with the functionality offered by CCN/CSI. A comprehensive overview of CCN/CSI is available in [RD1]

1.5 GUIDANCE TO READERS

The National Administrations are supposed to have been informed about the general principles of this document; however, they are invited to permanently assess that the policy statements contained in the document correspond to their understanding of the security model proposed. They may well wish to consult their national security advisors to discuss how the measures might be implemented. They should also confirm the basic assumptions, particularly those concerning the security services provided by the Community Domain network.

1.6 BASIC PRINCIPLES

This policy describes the essential principles and rules of CCN/CSI information security. Its purpose is to facilitate the achievement of CCN/CSI 's overall objectives through consistent and optimally protected information support. Although this document is a complete re-write, the basis for this information security policy is the general CCN/CSI security policies and guidelines. This policy is an introduction to and a foundation for more detailed standards and guidelines on Information and IT Security.

The CCN/CSI Information Security Policy is owned by DG TAXUD and maintained by the CCN/TC.

Its principles and rules, as well as instructions and guidelines derived from them, are recommended throughout the whole of CCN/CSI as minimum-security requirements.

Information and system owners may, according to the risks involved, install tighter security requirements and solutions.

Information about the compliance status of this policy and plans for its improvement are available through the document owner.

This document is sensitive and should only be distributed on a need-to-know basis, at the discretion of DG TAXUD.

The CCN/CSI Security Policy provides a set of high-level principles and objectives for information security together with associated statements of good practice. They can be used to improve the level of security in the following ways:

- Increase the information security level;
- Complement and strengthen business processes;
- Assess performance in information security;
- Support security audits/reviews;
- Enhance security awareness programs;
- Check compliance with industry standards;
- Provide authoritative reference material for particular initiatives.

Implementing the Policy will help to:

- Move towards inter-EU best practice;
- Manage the breadth and depth of information risk;
- Build confidence within the CCN/CSI community (NA, EC, CCN/TC) that information security is being addressed in a professional manner;
- Reduce the likelihood of disruption from major security related incidents;
- Maintain business integrity.

1.7 INFORMATION SECURITY AND IT SECURITY

Information is a business asset, which as with any other important asset, is valuable to the CCN/CSI framework and therefore needs to be sufficiently protected. The value of relevant and correct information to business is based on the following quality characteristics:

Confidentiality: Information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity: Information has not been corrupted, degraded, or undergone unauthorized modification.

Availability: Information is accessible and usable upon demand by an authorized user.

Accountability: Ability of a system to keep track of who or what accessed and/or made changes to the system.

Information security is the process of protecting the intellectual property of an organization. Its purpose is to reduce the information risk. Information security critically depends on people in order to be effective.

Breaches in information security lead to information leakage or shortages in information supply through errors and system breakdowns. These could cause both clearly visible and hidden damages.

The information security function aims at the preservation of information quality as far as is economically feasible. This implies seeking the balance between expected (probability weighted) business and image losses from insufficient security and the direct and indirect costs of information protection.

Relevance and correctness of the application data are outside the scope of information security in the Security Domain of the CCN/CSI network.

Discipline and control, data encryption, information and system multiplication, as well as backup arrangements and alternative procedures can protect information.

2 DOCUMENTS

2.1 APPLICABLE DOCUMENTS

Id	Reference	Title	Version
[AD1]	N/A	DG Taxation and Customs Union TEMPO Quality Methodology	N/A
[AD2]	DG TAXUD/A3/PHT/hc-D(2004) 62615	Request for Action (RFA) n°147	

2.2 REFERENCE DOCUMENTS

Id	Reference	Title	Version
[RD1]	CCN-COVW-GEN	CCN/CSI System Overview	EN12.00
[RD2]	CCN/CSI-EVOL-REQ-ATOR	CCNCSI Evolution Study – Requirements Analysis	EN3.00
[RD3]	CCN/CSI-EVOL-TCA-ATOR	CCNCSI Evolution Study – Technical/Costs Analysis	EN1.00
[RD4]	CCN-FES-SMTPA	SMTP implementation over CCN – Addendum to the Feasibility Study	EN0.20
[RD5]	CCN/CSI-DEP-MSA-01-MABX	NA Deployment Plan	EN4.00
[RD6]	CCN-CMPR-GW	Gateway Management Procedures	EN15.00
[RD7]	CCN-CSEC-RSKA	CCN/CSI Security Risks Assessment	EN1.00
[RD8]	CCN-CSEC-BSCK	CCN/CSI Baseline Security Compliance Checklist	EN1.00
[RD9]	CCN-CSEC-TCPRO	CCN/TC Security Procedures	EN1.00
[RD10]	ISO/IEC 17799: 2000	International Organization for Standardization/International Electro-technical Commission (ISO/IEC) 17799:2000, Code of Practice for Information Security Management.	N/A
[RD11]	ISF_Standard_2005.pdf	ISF: Standard of Good Practice	N/A
[RD12]	CCN-CNE-031	Procedure for the move of a CCN/CSI site	EN2.00
[RD13]	CCN-CSEC-PSCG	CCN/CSI Practical Security Guidelines	-TBW-

3 GLOSSARY

General CCN/CSI terms and acronyms are defined in the CCN/CSI Project Glossary, which is itself included in the CCN/CSI System Overview document [RD1]

3.1 SPECIFIC GLOSSARY OF TERMS

Asset An asset is a component or part of a total system to which the organisation directly assigns a value and therefore, requires protection. Assets encompass all of those items that contribute to the provision of information that an organisation requires in conducting its activity.

Audit Trail A record of events, such as system access, network load, unsuccessful logon attempts and so on, that might have some significance when investigating a security breach.

Authenticate Verify the identity of a communicating party.

Authorisation Permission to access data or a resource.

Availability The prevention of unauthorised withholding of information or resources.

Confidentiality The prevention of unauthorised disclosure of information.

Denial of service The prevention or interruption of a communication or the (unauthorised) delay of a time-critical operation.

Digital Signature A mathematical process that is applied to information, which can be used to assure the recipient of its authenticity with varying degrees of certainty.

Encryption A method of converting information into a form, which can be transmitted over insecure channels such as a LAN so that confidentiality is preserved.

End-user A person who makes direct use of (an IT system) capability.

Fraud Avoidance of payment of taxes and duties in full or in part or the claiming and obtaining of fictitious export refund claims.

Impact The undesirable consequence resulting from a security failure.

Integrity The prevention of unauthorised modification of information.

Security Objective The contribution to security that the system is intended to achieve.

Security Relevant That which is not security enforcing, but must function correctly for the system to enforce security.

System Security Policy The set of laws, rules, and practices regulating the processing of sensitive information and the use of the resources by the hardware and software of an IT system.

Threat An action or event, which might prejudice security.

Vulnerability A security weakness in a system, due to failures in requirement analysis, design, implementation, or operation.

Workstation Any terminal, PC or other device used to deliver the user interface to the CCN/CSI client application. This term is used in preference to the term "client" to avoid confusion with client processes, which may run on any of the platforms within CCN/CSI.

3.2 SPECIFIC GLOSSARY OF ACRONYMS

AP	Access Point
CBA	Critical Business Assets
CCN	Common Communication Network
CI	Computer Installations
CPR	Customer Premises Router
CSI	Common Systems Interface
DMZ	De-Militarised Zone
DSU	Data/Digital Service Unit
EC	European Commission
EU	European Union
IDA	Interoperable Delivery of European eGovernment Services to public Administrations
ISF	Information Security Forum
ISMS	Information Security Management System
ISO/IEC	International Standard Organisation/International Electrotechnical
ISO	Information Security Officer
LCMS	Local CCN Mail Server
LSA	Local Security Administrator
LSO	Local Security Officer
LSYA	Local System Administrator
NA	National Administration
NT1	Network Termination Device - Type 1 (ISDN)
NW	Networks
OLAF	European Anti-Fraud Office
PIN	Personal Identification Number.
SD	Systems Development
SM	Security Management
SRA	Security Risks Assessment
TC	Technical Center
WAN	Wide Area Network

4 CCN/CSI INFORMATION SECURITY OBJECTIVES

CCN/CSI must provide the CCN/CSI applications with a coherent set of generic security mechanisms that will help those applications to meet their own security objectives.

As corollary:

- CCN/CSI must provide a safe and trustworthy access and transport service to the client applications;
- CCN/CSI Generic Application Services (GAS) must provide a safe and trustworthy service to the client applications;
- By providing a single and coherent control mechanism of the basic security measures, CCN/CSI must guarantee a client application that security measures used by other client applications will not introduce new security vulnerabilities;
- CCN/CSI must protect National Administrations against intrusion via their CCN connection;
- CCN/CSI must prevent unauthorised access from a National Domain to the Common Domain.

The method used to reach that goal will be described in details in Section 7.

Headlines are given here for reference:

- Asset Risk Assessment (to define what needs protection);
- Risk Mitigation plan (to define how the risk to the identified assets will be brought to an acceptable level);
- Monitoring, Auditing and Review procedures (to make the process cycle upon itself according to the Plan-Do-Check-Act philosophy described in ISO/IEC 17799 [RD10].

5 SECURITY DOMAIN (CCN/CSI ARCHITECTURE OVERVIEW)

This section defines the components and jurisdiction of the Policy (logical and physical borders)

5.1 CCN/CSI COMPONENTS

The following components are the building blocks of a typical CCN/CSI site.

5.1.1 FIREWALLS

To isolate the various components of the CCN/CSI infrastructure, equipments embedding Firewall capabilities (packet filtering and/or circuit level gateways and/or application level gateways) shall be used.

These firewall type equipments shall separate the NA domain, the DMZ and the WAN, accessing them via three separate interfaces.

IP filters will be implemented in order to accept only authorised applications from and/or to authorised sites.

The firewall access control list (ACL) will be configured following the default "deny" principle: **That which is not expressly permitted is prohibited**

The list of the port numbers that are used by CCN/CSI applications will be provided by the CCN/TC.

In practice, the NetScreen boxes fulfil this functionality.

5.1.2 GATEWAYS (CSI ACCESS SERVERS)

As an additional step in the site protection, the CCN/CSI gateway only listens to a restricted amount of authorised applications and is securely configured.

Full description of the Gateways is to be found in the "Gateway Management Procedures" [RD6].

5.1.3 LCMS (MAIL SERVICE SERVERS)

The LCMS (CCN Mail2) offers an inter-personal messaging system relying upon the CCN/CSI network infrastructure and upon a collection of SMTP-based LCMS servers deployed in each country accessing the system.

Full description of the LCMS is to be found in the "SMTP implementation over CCN – Addendum to the Feasibility Study" document [RD4].

5.1.4 ROUTERS, HUBS, SWITCHES AND CABLING

Other elements of the network infrastructure are not to be overlooked.

These include but are not limited to routers, switches, hubs, bridges and even cables.

These elements should be documented and included in the scope of the auditing process.

5.1.5 VPN AND OTHER TUNNELLING EQUIPMENT

To ensure the Confidentiality and Integrity of the information transmitted over unsecured links, the CCN/CSI will rely on encryption devices building secure tunnels.

The VPN box is a first step in the protection of a CCN/CSI site (when looked at from the WAN end): it only accepts encrypted packets from other CCN/CSI sites that are also equipped with a VPN box.

In practice, the NetScreen boxes fulfil this functionality.

5.1.6 WAN TRANSPORT PROVIDER

Last but not least the WAN transport provider completes the overall picture of the Security Domain.

It isn't responsible for Confidentiality and Integrity (as it is taken care of by the VPN equipment) but the Availability is clearly of its responsibility.

5.2 CCN/CSI BORDERS

By CCN/CSI borders and therefore jurisdiction, is meant the territory both physical and logical where the responsibility of the CCN/CSI applies.

5.2.1 EURO DOMAIN

The *EuroDomain* is composed of all the computer equipment (communication lines included), making up the CCN network, including the CCN/CSI DMZ, the technical operation, monitoring and security centres.

5.2.2 NATIONAL ADMINISTRATION DOMAINS

The *National Domain* is composed of all the computer equipment peculiar to a National Administration (communication lines included), up to the CCN/CSI DMZ.
In terms of IDA terminology, a national domain is a Local Domain (LD); DG TAXUD is also a Local Domain and is assimilated to a National Domain throughout this document.

The CCN gateway DMZ is located at the border of the two domains.

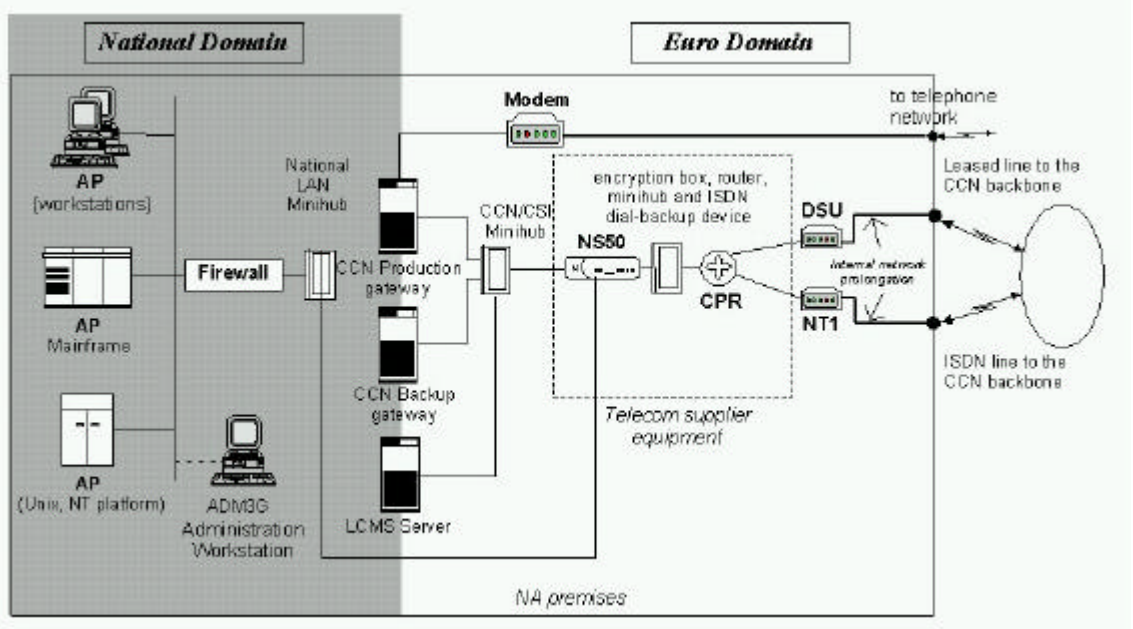

FIGURE 1: CCN/CSI ARCHITECTURE OVERVIEW

6 PARTIES AND RESPONSIBILITIES

6.1 INFORMATION AND SYSTEM OWNERS

DG TAXUD is the owner of the information, services and data processing systems in CCN/CSI. The CCN/TC operates the CCN/CSI infrastructure on behalf of DG TAXUD.

The principal security responsibilities of the owner are:

- Definition and approval of security requirements for the information or system;
- Approval of information users and their usage rights;
- Decisions upon level and cost of information and system protection that reduce the information risk to an acceptable level;
- Delegation of responsibilities for the activities above.

6.2 USERS AND MANAGERS

Users is a broad term describing ALL persons or applications with access to the information and processing systems that work within the limits of security solutions and rules. As there always will be freedom to act also in an insecure way the self-discipline and integrity of Users are essential.

CCN/CSI Users are persons or applications having access to the CCN/CSI transport services.

CCN/TC Registered Contacts are people registered by the CCN/TC as official contact points authorised to access the CCN/TC services. This avoids that unauthorised persons request for CCN/TC interventions.

CCN/CSI Managers roles of the National Administrations are listed below. It must be stressed that DG TAXUD and OLAF are assimilated to National Administrations for any issues related to the local domain, i.e. the connection of the application platforms to the CCN gateways and LCMS, and the part of administration that they have to perform on these CCN machines.

Role	Description
TPM Technical Project Manager	Responsible and liaison with DG TAXUD and other NAs for all CCN/CSI technology issues.
APM Administrative Project Manager	Responsible and liaison with DG TAXUD and other NAs for all CCN/CSI administrative issues.
LSO Local Security Officer	Responsible for the overall CCN/CSI-related security measures according to the CCN/CSI security policy, including user access rights. The LSO will be appointed by the NA.
LAA Local Application Administrator	Responsible for: CCN/CSI Users registration; Limited user management, i.e. handling all CCN/CSI user profiles (or only part of them) defined for a given application domain.
LSA Local Security Administrator	Responsible for: Update application security keys; CCN/CSI Users registration; Extended user management, i.e. handling all CCN/CSI user profiles available at the local site Directory management, i.e. browse Directory, view replication agreements, refresh CCN Directory cache.
LSYA Local System Administrator	Responsible for executive work on behalf of the Central System Administrator (CCN/TC) for the administration of the CCN/CSI gateway and LCMS hosted in the premises of the NA, and responsible for the system management of the CSI software in the National Domain, according to the CCN/CSI Security Policy
Local Network Administrator	Responsible for the network connections inside the National Domain
Installer	Responsible for the software installation and maintenance

TABLE 1: CCN/CSI MANAGERS ROLES OF THE NATIONAL ADMINISTRATIONS.

6.3 CCN/CSI SQUARE MODEL

The CCN/CSI community has adopted a so-called “Square Model” to organise the operations and support activity (Figure 2: “Square Model” Organisation.). This model implies that the end-user of an application using the services offered by CCN/CSI can only call for the Local Application Support provided by its Administration.

The Local Application Support can ask for services offered by the Local CCN/CSI support (e.g. a request to solve an incident related to the CCN/CSI infrastructure or a request to define new users in the CCN directory). However, the Local Application Support cannot directly call the CCN/TC, for the same reason as a final user cannot directly call the Central Application Support.

The Local Application Support can, of course, call for the services of the Central Application Support and the Central Application Support can also call for services provided by the Local Application Support (e.g. local installation of application software developed centrally).

In the same way, the Local CCN/CSI Support can of course call for the CCN/TC services, and vice versa. For example, the CCN/TC will have to call for the Local CCN/CSI Support to validate new versions of CSI, or to install new versions of CSI on the application platforms.

The Central Application Support entities can also call for the CCN/TC services. This will be the case when defining new application messages, new services and application queues or new user profiles.

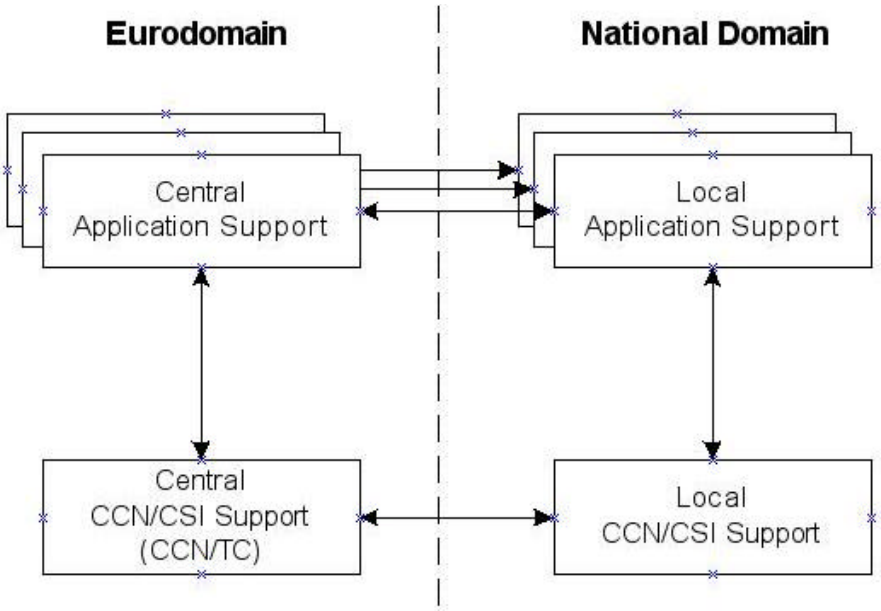

FIGURE 2: "SQUARE MODEL" ORGANISATION.

6.4 NATIONAL ADMINISTRATIONS RESPONSIBILITIES

6.4.1 SYSTEM ADMINISTRATION

Each National Administration must provide a service to manage the authorisations of their CCN/CSI client applications in the CCN/CSI directory on the CCN/CSI gateway and on any complementary platform.

Local IT administrators must be granted access only to those services necessary to do their job. The list of services provided must be chosen so that the rights and privileges conferred cannot be exploited to circumvent the security controls.

Local IT administrators may not change the gateway configuration, except the National Domain identifications and usage rights in the directory. Gateway configuration is allocated to the CCN/CSI Technical Centre.

The list of authorised applications and users, and the services to which they have been granted access must be subject to regular reviews.

Rights and privileges must be granted only in accordance with well-defined rules regarding segregation of duties.

6.4.2 TRAINING

National Administrations should initiate an on-going IT security awareness programme for IT administrators and CCN/CSI applications developers.

6.4.3 SYSTEM SECURITY POLICY

Each National Administration should rely on the CCN/CSI Security Policy for their National systems connecting to the CCN/CSI gateway.

The system security measures implemented may be validated as part of the certification process.

A typical outline of security measures is provided in the Baseline Security Checklist document [RD8] and in the Practical Security Guidelines document [RD13].

6.4.4 SECURITY OPERATING PROCEDURES

Each National Administration should document the measures implemented to manage their CCN/CSI access in a secure manner. Compliance with them should be tested as part of the Initial Operational Assessment and periodically thereafter.

6.4.5 CCN SITE MOVE PROCEDURE

Whether a National Administration intends to move its CCN/CSI site to another location, a dedicated procedure has to be followed. This procedure [RD12] defines the steps involved in a move of a CCN/CSI site, the different tasks that need to be performed and the timeframe needed to successfully complete the action. The successful achievement of the move depends of the close coordination between the administration responsible and the CCN/TC who will

act as a co-ordinator with regards to DG TAXUD, the CCN gateways and LCMS supplier and the WAN provider.

The CCN site move procedure is available on the CCN/TC web site or can be requested by email directly to the CCN/TC.

6.4.6 THE TEN CCN COMMANDMENTS

The National Administrations responsibilities are often summarised by the following "ten CCN commandments" list:

1. NA should provide the names of their contacts to the CCN/TC and notify any modification;
2. NA should ensure a continuous presence for the CCN/CSI administration during working hours;
3. CCN gateways, LCMS, security and telecom equipment should be properly housed (storage place, power supply, ...);
4. CCN gateways, LCMS, security and telecom equipment should be properly maintained (daily backup of gateways, ...);
5. CCN gateways, LCMS, security and telecom equipment should never be stopped without formal authorisation from the CCN/TC;
6. The CCN/TC should be notified of any problems impacting the CCN gateways, LCMS, security and telecom equipment or the CCN services;
7. NA should provide a secure environment for the CCN gateways, LCMS, security and telecom equipment;
8. NA should collaborate with the CCN/TC and grant physical access to the equipment when required;
9. Authorisation from the European Commission is requested prior to install additional hardware or software on the CCN gateways, LCMS, security and telecom equipment;
10. NA should disseminate these commandments to the CCN/CSI staff.

7 CCN/CSI INFORMATION SECURITY MANAGEMENT SYSTEM

7.1 SECURITY FRAMEWORK

7.1.1 DESCRIPTION OF THE STANDARD USED (AND THE REASON THEY ARE)

To tackle the Information Security issue consistently, one needs to develop a structured framework covering all needed aspects and giving the possibility to fulfil management requests as well as help the field people implement security following an "easy to understand" model.

Relying on International Standards is beneficial, as it will help the CCN/CSI to:

- Move towards international best practice;
- Manage the breadth and depth of information risk;
- Build confidence in third parties that information security is being addressed in a professional manner;
- Reduce the likelihood of disruption from major incidents;
- Fight the growing threats of cyber crime;
- Comply with legal and regulatory requirements;
- Maintain business integrity.

The ISO/IEC 17799 Standard has been prepared for business managers and their staff to provide a model for setting up and managing an effective Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by business needs and objectives, resulting security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that simple situations require simple ISMS solutions.

From an industry perspective, ISO/IEC 17799 has come under some criticism for being too general, but it is being adopted by many companies - and is the only international standard covering information security. Because of this lack of "practicality", it was decided to use also a standard developed by and for the industry: ISF2005.

The ISF standard has been produced by the Information Security Forum (ISF), an international association of over 260 leading organisations, which fund and co-operate in the development of a practical research programme in information security. During the last 16 years the ISF has spent more than US$75 million providing authoritative material to its Members. The ISF's work probably represents the most comprehensive and integrated set of material anywhere in the world in the area of information risk management.

Therefore it appeared beneficial to use a blend of these two standards:

- The ISO/IEC 17799 Standard [RD10];
- The Information Security Forum (ISF) practical guidance 2005 [RD11].

7.1.2 ISO/IEC 17799 DESCRIPTION

The ISO/IEC 17799 International Standard (ISO/IEC) provides a comprehensive approach to the management of information system security. It is based on the British Standards Institution BS 7799 Part 1 (BSI).

This ISO Standard can be used by internal and external parties including certification bodies, to assess an organization's ability to meet its own requirements, as well as any customer or regulatory demands.

It is organised into 10 major sections, each covering a different topic or area:

7.1.2.1 SECURITY POLICY

The objective of this section: to provide management direction and support for information security.

7.1.2.2 SECURITY ORGANIZATION

The objectives of this section:

- To manage information security within the CCN/CSI;
- To maintain the security of organizational information processing facilities and information assets accessed by third parties;
- To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

7.1.2.3 ASSET CLASSIFICATION AND CONTROL

The objectives of this section: to maintain appropriate protection of CCN/CSI assets and to ensure that information assets receive an appropriate level of protection.

7.1.2.4 PERSONNEL SECURITY

The objectives of this section:

- To reduce risks of human error, theft, fraud, or misuse of facilities;
- To ensure that users are aware of information security threats and concerns and are equipped to support the CCN/CSI security policy in the course of their normal work;
- To minimise the damage from security incidents and malfunctions and learn from such incidents.

7.1.2.5 PHYSICAL AND ENVIRONMENTAL SECURITY

The objectives of this section:

- To prevent unauthorised access, damage and interference to CCN/CSI premises and information;
- To prevent loss, damage, or compromise of assets and interruption to CCN/CSI activities;
- To prevent compromise or theft of information and information processing facilities.

7.1.2.6 COMPUTER AND NETWORK MANAGEMENT

The objectives of this section:

- To ensure the correct and secure operation of information processing facilities;
- To minimize the risk of systems failures;
- To protect the integrity of software and information;
- To maintain the integrity and availability of information processing and communication;
- To ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
- To prevent damage to assets and interruptions to CCN/CSI activities;
- To prevent loss, modification or misuse of information exchanged between organizations.

7.1.2.7 SYSTEM ACCESS CONTROL

The objectives of this section:

- To control access to information;
- To prevent unauthorised access to information systems;
- To ensure the protection of networked services;
- To prevent unauthorized computer access;
- To detect unauthorised activities;
- To ensure information security when using mobile computing and telenetworking facilities.

7.1.2.8 SYSTEM DEVELOPMENT AND MAINTENANCE

The objectives of this section:

- To ensure security is built into operational systems;
- To prevent loss, modification, or misuse of user data in application systems;
- To protect the confidentiality, authenticity, and integrity of information;
- To ensure CCN/CSI projects and support activities are conducted in a secure manner;
- To maintain the security of application system software and data.

7.1.2.9 BUSINESS CONTINUITY PLANNING

The objectives of this section: to counteract interruptions to business activities and critical business processes from the effects of major failures or disasters.

7.1.2.10 COMPLIANCE

The objectives of this section:

- To avoid breaches of any criminal or civil law, statutory, regulatory, or contractual obligations and of any security requirements;
- To ensure compliance of systems with CCN/CSI security policies and standards;
- To maximize the effectiveness of and to minimize interference to/from the system audit process.

7.1.3 ISF MODEL DESCRIPTION

The Standard focuses on how information security supports an organisation's key business processes. These processes increasingly depend on IT-based business applications, many of which are critical to their success. Thus the aspect of security concerned with Critical Business Applications is central to the design of the Standard.

The Standard of Good Practice is split into five distinct containers, each of which covers a particular type of environment.

- Security Management (SM);
- Systems Development (SD);
- Computer Installations (CI);
- Networks (NW);
- Critical Business Assets (CBA).

Computer Installations and Networks provide the underlying infrastructure on which the Critical Business Applications run. Systems Development deals with how new applications are created and Security Management addresses high-level direction and control.

7.2 RISK MANAGEMENT

7.2.1 RISK ASSESSMENT

The Security Risks Assessment (SRA) is a fundamental step in the establishment and implementation of a logical and systematic program for information security management involving the whole CCN/CSI community.

It aims at identifying what are the "real" Security Risks to the CCN/CSI assets, and what Security Measures, whether technical or procedural, are appropriate to eliminate (or at least to reduce) the identified risks, so as to ensure the continuity of the CCN/CSI business.

To reach this goal, it is necessary to:

- Describe the CCN/CSI components model to be considered, and to inventory the CCN/CSI assets, i.e. the value to be protected;
- Gain an understanding of the security risks by:

  Creating an inventory of and evaluating the threats to CCN/CSI assets;

  Analysing the level of vulnerability of CCN/CSI assets to the identified threats;

  Evaluating the impact of each threat to the CCN/CSI business (in the case it were to occur).

Each identified risk is then evaluated (on a scale from 1 to 3) according to the reference and the resulting **Master Risks List** is used to develop the Risk Mitigation Plan.

7.2.2 RISK MITIGATION PLAN

The Risk Assessment process identifies the threats and defines the Risk Level to CCN/CSI Assets.

The Risk Mitigation Plan is the expression of security measures definition and implementation planning. It aims at reducing the Risk level

7.2.3 SECURITY MEASURES MATRIX

The Measure Matrix is the tool that allows dispatching the Security Measures across the whole security framework

It allows cross working with ISO17799 standard, with ISF container model, with the Risk Levels defined in the Risk Assessment and with the Square Model,

It is merely a database of practical security measures that can be sorted according to the needs of the various Security responsibles.

As an example:

- Security Officer and LSO will be working with the Risk Level and the ISF indexes;

- Local Security and National Administration teams will rely on the Risk Level and the Measure's definition to comply with the Baseline Security Compliance Checklist [RD8] according to the process described in Appendix A. CCN/CSI Security Compliance Process.

7.2.4 MONITORING – AUDITING – REVIEWING

When the Security Measures have been applied, the CCN/CSI Security Authorities need to be aware of the actual security status of the concerned Security Domain. Therefore after completing the Risk Assessment phase (to define the assets inventory and risks threatening these assets) and the Risk Mitigation phase (to apply Security Measures to the assets to control the risks identified), there is a need for three additional processes:

- Monitoring: to ensure smooth operation level and spot vulnerabilities and/or attacks.
- Auditing: to ensure by external scrutiny that the Security Policy is applied consistently, Risk Assessment in line with the reality and Risk Mitigation performed adequately.
- Review: to apply the updates required by Security Policy evolution or the recommendations from Monitoring and Audit reports.

The purpose of this section is to define, in terms of responsibility and planning, how these three fundamental tasks will be fulfilled.

7.2.4.1 MONITORING

The Security Officer will apply the required monitoring measures necessary to ensure smooth operation level and spot vulnerabilities and/or attacks. The detail of these measures will be defined in the Baseline Security Checklist [RD8] (for the NAs) and in the CCN/TC Security Procedures [RD9] (for the CCN/TC). Some practical measure's implementation examples will be given in the Practical Guidelines documents [RD13].

7.2.4.2 AUDITING

The ultimate goal of the Auditing process is to give a very clear vulnerability status of the Security Domain.

[**Note**: Scope and periodicity of the audits is to be defined by TAXUD]

A first thorough audit of the whole infrastructure should be performed to assess its current vulnerability status.

Further audits could be more specific in physical and/or logical scope (area of responsibility, location, device type, network component…).

7.2.4.3 REVIEW

The deliverables produced by the Monitoring and the Auditing processes will be submitted to the Security Council and will be used to improve the Policy.

8 APPENDIX A. CCN/CSI SECURITY COMPLIANCE PROCESS

8.1 HOW TO LAUNCH THE SECURITY COMPLIANCE PROCESS

Local Security Officers must establish an overall plan to implement the Information Security Procedures. Performing the following three-step process will result in a completed Security Compliance Certification for the area under review.

STEP 1: Establish the scope and depth of Security Compliance Process

Identify major business/administrative functions (at site level).

Identify information assets within each business/administrative function.

Identify/inventory application systems within each business/administrative function (in some small sites case, the inventory can be done at site level).

Prioritise assets/systems based upon initial perceived risk.

STEP 2: Risk Assessment Phase

Establish the business owner for each system/application/informational asset.

In conjunction with the Owner, assess Threat and Vulnerability related to each Asset.

Put the Risk ratings into a worksheet to obtain required protection ratings for the Asset.

STEP 3: Risk Mitigation Phase

Prepare a gap analysis, for each Asset in question, relating to the "CCN/CSI Security Compliance Checklist" versus existing controls.

Prepare a Risk Mitigation Plan based on the Assets gap analysis including cost of implementing required controls and specific timelines for implementation.

The Risk Mitigation Plan can be implemented by Site or at the CCN level as desired by CCN/CSI and DG TAXUD management and according to economies of scale.

Obtain the authorization of the NA authorities to proceed with Risk Mitigation Plan implementation.

If local management will not authorize all required controls then obtain a waiver and send along to CCN/TC for review and approval.

Implement the approved Risk Mitigation Plan.

Monitor and re-assess as necessary, but at a minimum when major changes occur in the business function, organization, systems or facilities supporting the business functions.

END OF DOCUMENT