ORIGINATOR:	ISSUE DATE:	VERSION:
ATOS ORIGIN	14-Jun-2006	EN2.00

TAXATION AND CUSTOMS UNION DG

CCN/CSI Project

SUBJECT:

CCN/CSI BASELINE SECURITY CHECKLIST

CCN-CSEC-BSCK

FRAMEWORK CONTRACT TAXUD/00/C063
SPECIFIC CONTRACTS 18

DOCUMENT HISTORY

Edi.	Rev.	Date	Description	Action (*)	Paragraphs
0	01	30-May-2005	Creation	I	All
0	02	02-Jun-2005	Internal Quality Review	I	All
0	10	03-Jun-2005	Official version sent for review		None
0	11	9-Feb-2006	Taking into account DRF_RFA147_CCN-CSEC-BSCK-EN0.10.doc	I, R	All
0	12	10-Feb-2006	Internal Quality Review	I, R	All
0	20	10-Feb-2006	Official Version sent for Review		None
1	00	13-Feb-2006	Official Version Sent for Acceptance		None
1	01	01-Jun-2006	Taken into account TAXUD comments on CCN-CSEC-RSKA	I, R	§4.1.7, §4.2.5, §4.2.7, §4.2.9, §4.3.8
1	10	09-Jun-2006	Official Version Sent for Review		None
2	00	14-Jun-2006	Official Version Sent for Acceptance		None

(*) ACTION: I=INSERT R=REPLACE

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE OF THIS DOCUMENT

This document defines the Baseline Security Procedures for the CCN/CSI infrastructure.

More than just depicting general security principles, it provides a checklist of security procedures for CCN/CSI to apply, covering the 10 ISO 17799 chapters:

1. Security Policy
2. Security Organization
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Computer and Network Operations
7. System Access Control
8. System Development and Maintenance
9. Business Continuity Planning
10. Compliance

Each of these chapters is further divided accordingly to the ISF container model

1. Security Management (SM)
2. Systems Development (SD)
3. Computer Installations (CI)
4. Networks (NW)
5. Critical Business Applications (CBA)

For more detailed information regarding these Security Standards, please refer to [RD9] and [RD10].

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	Baseline Security Checklist This section describes the CCN/CSI Baseline of Security Procedures, presented as checklists of steps to be taken in order to satisfy the CCN/CSI security expectations.

1.3 FIELD OF APPLICATION

The present document is applicable for operational usage of the CCN/CSI infrastructure.

1.4 INTENDED AUDIENCE

The intended readership for this document includes:

- Those responsible for designing and implementing CCN/CSI security features into the CCN/CSI local sites;
- Those responsible for the definition of the functional and technical specification of CCN/CSI.

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 CCN/CSI involved parties are supposed to know the general principles of this document. The Security involved parties as defined in [RD8] are invited to permanently assess that the policy statements contained in the document correspond to their understanding of the threats and the relevance of the measures proposed.

1.6 BASIC PRINCIPLES

This set of practical procedures describes the essential steps to be performed in order to achieve the required Baseline CCN/CSI information security level.

The sets of measures presented in section 4 are extracts out of a matrix of generic procedures.

As a first step, only the measures that correspond to the risk level (meaning by that “needed to mitigate the risk”) defined by the Risk Assessment [RD7] are selected.

After that, the set of measures is split in parts to eliminate the measures specific to the CCN/TC and to separate the measures according to the Square model.

The result thereof is a number of tailor-made security measures sets appropriate for the NAs.

Its purpose is to facilitate the achievement of CCN/CSI's overall objectives through consistent and optimally protected information support.

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

Information and system owners may, according to the risks involved, set-up higher security requirements and solutions.

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

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

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	EN11.00
[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	EN1.00
[RD6]	CCN-CMPR-GW	Gateway Management Procedures	EN14.00
[RD7]	CCN-CSEC-RSKA	CCN/CSI Security Risks Assessment	EN0.10
[RD8]	CCN-CSEC-POL	CCN/CSI General Security Policy	EN0.10
[RD9]	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
[RD10]	ISF_Standard_2005.pdf	ISF: Standard of Good Practice	N/A

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.
CCN/CSI Security	The security of the CCN/CSI network infrastructure
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.
Evidence	Something that supports a claim or hypothesis.
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.
Third-parties	Entities external to the CCN/CSI but conducting business implying access and exchange of data with it.
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

CA	Certificate Authority (PKI)
CBA	Critical Business Assets
CCTA	Central Computer and Telecommunications Agency (UK)
CI	Computer Installations
CRAMM	CCTA Risk Analysis and Management Method
ISF	Information Security Forum
ISMS	Information Security Management System
ISO/IEC	International Standard Organisation/International Electrotechnical Commission
ISO	Information Security Officer
NDA	Non-Disclosure Agreement
NW	Networks
RSKA	RiSK Assessment
SD	Systems Development
SM	Security Management

4 BASELINE SECURITY CHECKLIST

4.1 MEASURES COMMON TO BOTH LOCAL CCN SUPPORT (LOCCCN) AND LOCAL APPLICATION SUPPORT (LOCAPP)

4.1.1 SECURITY POLICY

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
101	SecPol	Management involvement	Management commitment to security must be well publicized at the site and business level.	1	SM	1	x	x	x	x
103	SecPol	Publication of Advisories	Security advisories must be posted by LSOs in a manner that ensures that all users who may be affected have access to these documents.	1	SM	1	x	x	x	x
104	SecPol	Third parties adhere to CCN/CSI policy	Third-party agreements should comply with the CCN/CSI General Security Policy.	1	SM	1	x	x	x	x

TABLE 1: COMMON MEASURES WITH REGARD TO SECURITY POLICY.

4.1.2 SECURITY ORGANIZATION

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
204	SecOrg	LSO must exist at site level	Local Security Officers must be established by their NA, as required by the CCN/CSI General Security Policy (section 6.2), to provide pertinent information to all system users during new-user orientations and to provide security briefings and retraining.	2	SM	1	x	x	x	
205	SecOrg	Reporting from LSO to local support and CCN/TC	Local Security Officers (LSOs) must report incidents to NA management and CCN/TC ISO in accordance with CCN/CSI General Security Policy.	2	SM	1	x	x	x	
207	SecOrg	User communication about backup needs	Users must understand the need for, and methods of, backing up files (under their control) on a scheduled basis and be knowledgeable concerning the methods of backing up files.	2	SM	1	x	x	x	x
208	SecOrg	Information owners must review data access rights	Information Owners (on behalf of CCN/CSI and as defined by the CCN/CSI General Security Policy) must review system and application privileges on a periodic basis (at least twice a year for Risk Level 3, and once per year for Levels 2 and 1).	2	SM	1	x	x	x	x

TABLE 2: COMMON MEASURES WITH REGARD TO SECURITY ORGANISATION.

4.1.3 ASSET CLASSIFICATION AND CONTROL

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
301	AssetC&C	Information owners must review asset classification	Information Owners (on behalf of CCN/CSI and as defined by the CCN/CSI General Security Policy) must review assets risk level classification on a periodic basis (e.g. twice per year for Risk Level 3, and once per year for Levels 2 and 1).	2	SM	1	x	x	x	x
303	AssetC&C	Authorisation to disclose confidential data	Proper authorization must be obtained from DG TAXUD for disclosure of CCN/CSI information (especially for third parties)	3	SM	1	x	x	x	x

TABLE 3: COMMON MEASURES WITH REGARD TO ASSETS CLASSIFICATION AND CONTROL.

4.1.4 PERSONNEL SECURITY

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
402	PersoSec	Third parties must warn CCN/CSI of personnel changes	Third parties must notify CCN/CSI of all personnel changes affecting CCN/CSI accounts.	4	SM	1	x	x	x	x
409	PersoSec	Information security education and training	All members of the organization and, where relevant, third-party users, shall receive appropriate training and regular updates in organizational policies and procedures.	4	SM	1	x	x	x	x
410	PersoSec	Reporting security incidents	Security incidents shall be reported through the Square Model escalation and reporting chain as quickly as possible. Further details will be placed in the Incident Response Procedure.	4	SM	1	x	x	x	x
411	PersoSec	Reporting security weaknesses	Users of information services shall be required to note and report any observed or suspected security weaknesses in, or threats to, systems or services.	4	SM	1	x	x	x	x
412	PersoSec	Reporting software malfunctions	Procedures shall be established for reporting software malfunctions.	4	SM	1	x	x	x	x
413	PersoSec	Learning from incidents	Mechanisms shall be put in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored. These mechanisms should be referenced by the Incident Response Procedure.	4	SM	1	x	x	x	x

TABLE 4: COMMON MEASURES WITH REGARD TO PERSONNEL SECURITY.

4.1.5 PHYSICAL AND ENVIRONMENTAL SECURITY

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
503	PhysSec	Badge mandatory	All NA members and contractors must be identified by security badges. Where Level 3 assets are at risk, ID badges must be worn at all times.	5	SM	1	x	x	x	x
504	PhysSec	Hosts for visitors	Visitors must be hosted by a NA member, have their identities authenticated, and be given temporary identification badges when accessing CCN/CSI facilities.	5	SM	1	x	x	x	x

TABLE 5: COMMON MEASURES WITH REGARD TO PHYSICAL AND ENVIRONMENTAL SECURITY.

4.1.6 COMPUTER AND NETWORK OPERATIONS

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
601	ComNet Ops	No installation of unauthorized software	Installation of unauthorized software should be prohibited and technically enforced where possible.	6	CI	1	x	x	x	x
607	ComNet Ops	No hardware hook-up to the Network without approval	Unapproved hardware shall not be connected to the CCN/CSI internal network without the approval of CCN/CSI Security Officer	6	NW	1	x	x	x	x

TABLE 6: COMMON MEASURES WITH REGARD TO COMPUTER AND NETWORK OPERATIONS.

4.1.7 SYSTEM ACCESS CONTROL

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
701	AccessCtrl	Access control must be enforced	System configurations (mobile, remote, and network connected) must not allow unauthorized access to CCN/CSI information and computing resources.	7	CI	1	x	x	x	x
704	AccessCtrl	All confidential data must be protected	For all systems containing confidential, personally identifiable data, access must be properly logged and protected on a need to know/do basis.	7	CI	2	x	x	x	x
710	AccessCtrl	Report access abuse	Report in an immediate and urgent manner any attempt at unauthorized use of identification codes and passwords to the Local Security Officer.	7	SM	1	x	x	x	x
715	AccessCtrl	Logon banners	Logon banners must be in place to notify users that system use is for authorized personnel only and that their activities may be monitored. Banners must notify the user that further use of the system implies consent to monitoring and that appropriate action will be taken for misuse of CCN/CSI systems (in accordance with applicable CCN/CSI policy and/or local law or regulation).	7	CI	1	x	x	x	x
716	AccessCtrl	Granularity of access right on NTK/NTD basis	Network & application access controls must provide adequate security functionality (e.g. ability to create, edit, display) so that access is granted to users on a need to know/do basis.	7	CI	1	x	x	x	x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
718	AccessCtrl	Protection of confidential data in transfer between applications	Confidential Information passed between application systems must be properly protected during transfer and by all applications that use or process the information (e.g. encryption).	7	CI	2	x	x	x	x
719	AccessCtrl	Change default passwords	Default vendor IDs (admin/admin) and guest/generic/group IDs (or any single ID that is used by more than one individual) should either be removed or disabled on all systems, including network operating systems (NOS), software applications, databases (DB), network equipment, etc.	7	CI	1	x	x	x	x
720	AccessCtrl	Detect misuse of passwords	Safeguards must be implemented to detect any attempt at unauthorized use of identification codes and/or passwords (e.g. logging and account locking).	7	CI	1	x	x	x	x
721	AccessCtrl	Password structure	Passwords must be of sufficient length and strength to deflect brute-force cracking attempts. E.g., passwords must have a length of 8 characters and one non-alpha numeric character (example, *, ?, &, etc.) in other than the last two characters of the password. Passwords must be changed/expired at least every 120 days. Applications that can accept network authentication can do so (e.g., single sign-on).	7	CI	1	x	x	x	x
722	AccessCtrl	Password not being personal user data	Personal information should not be used as userids or passwords.	7	CI	1	x	x	x	x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
723	AccessCtrl	Password stored encrypted	Systems must maintain and store passwords in an encrypted format.	7	CI	1	x	x	x	x
724	AccessCtrl	Password history of 12 months	Network passwords must not be repeated for 12 months or an equivalent number of iterations depending on operating system.	7	CI	1	x	x	x	x
729	AccessCtrl	Power on password on laptops	Portable computers (including laptops and PDAs) must use power-on and/or hard drive passwords and, if available, inactivity timeouts (e.g., screen saver) of 15 minutes or less.	7	CI	1	x	x	x	x
730	AccessCtrl	Authentication token not to be stored with device	Tokens must not be stored with the computing device (e.g. Access badges are not to be stored next to the access control device that opens the lock of the door. Otherwise, anybody could take the “token” and activate the “device”).	7	CI	1	x	x	x	x
733	AccessCtrl	Service accounts must not be interactive	Where technically possible, service accounts (e.g. Tuxedo, LDAP) should not permit interactive (console) login from the OS command line, (e.g. In Unix, users should be forced to login to a unique named personal account on a given computer and then may "switch-user" to a general or service type account).	7	CI	1	x	x	x	x
734	AccessCtrl	Service account scope restriction	The scope of control/access for such accounts must be restricted to only the server(s) and/or applications required.	7	CI	1	x	x	x	x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
738	AccessCtrl	Audit trails able to identify the user	Procedures and controls must be designed and implemented for audit trails to be able to identify the user who created or modified a document or record.	7	CI	1	x	x	x	x
744	AccessCtrl	Audit trails retention period	Application audit trail records must be maintained for at least as long as the retention of the underlying files.	7	CI	2	x	x	x	x
749	AccessCtrl	Date/time stamp independent from users	The date/time must be independently recorded (i.e., not configurable by the user) to guarantee the validity of the logs.	7	CI	2	x	x	x	x
757	AccessCtrl	Usage of crypto tools requires project owner approval	Deployed cryptographic products should use non-proprietary crypto-algorithms and key lengths authorized by EU law and/or any applicable local laws. Cryptographic products (proprietary and non-proprietary) implemented for production work must be approved by CCN/CSI Security.	7	SM	1	x	x	x	x
759	AccessCtrl	Secure data transmission over insecure networks	Information and programs communicated via an entrusted, external network should be adequately protected from modification and disclosure (e.g. encryption, digital signatures, checksums/hash totals, etc.).	7	CI	2	x	x	x	x
764	AccessCtrl	External < Internal /access	Non-CCN/CSI personnel (e.g. vendors, consultants, and contractors) must have at least the same access restrictions to which an internal user is subject.	7	SM	2	x	x	x	x
765	AccessCtrl	Info access restriction NTK	Non-CCN/CSI personnel must be restricted to the information required to complete the contracted work.	7	SM	2	x	x	x	x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
766	AccessCtrl	Wireless network products security	Wireless network products, including those used for email (e.g., Blackberry-type devices), must use authentication and encryption mechanisms approved by CCN/CSI Security. These devices must use a power-on password plus an inactivity time-out of 15 minutes or less.	7	CI	2	x	x	x	x

TABLE 7: COMMON MEASURES WITH REGARD TO SYSTEM ACCESS CONTROL.

4.1.8 SYSTEM DEVELOPMENT AND MAINTENANCE

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
881	SysDev&M	Procedure for testing of security patches	Operating and maintenance procedures must be implemented to ensure that operating system and application security patches are tested and applied when received from vendors.	8	CI	1	x	x	x	x
882	SysDev&M	Backups before applying changes	Appropriate system, application, and data backups should be performed before any upgrade or maintenance occurs, ensuring the ability to revert to the state prior to changes.	8	CI	2	x	x	x	x

TABLE 8: COMMON MEASURES WITH REGARD TO SYSTEM DEVELOPMENT AND MAINTENANCE.

4.1.9 BUSINESS CONTINUITY PLANNING

Id	Field	Security Measure	Description	ISO	ISF	Risk	Square Model Applicability

							LocApp	LocCCN	CenlApp	CCN/TC
913	BusiCont	Logging of Incidents and Responses	A summary record of all incidents and actions taken must be maintained in a secure fashion.	9	SM	1	x	x	x	x

TABLE 9: COMMON MEASURES WITH REGARD TO BUSINESS CONTINUITY PLANNING.

4.1.10 COMPLIANCE

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
1002	Compliance	NDA when possible	Where permitted by law, CCN/CSI members, temporary employees, consultants and vendors must sign a confidentiality and non-disclosure agreement which, at minimum, requires them to safeguard CCN/CSI confidential and proprietary information.	10	SM	1	x	x	x	x
1004	Compliance	Intellectual property rights protection	Appropriate procedures shall be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products.	10	SM	1	x	x	x	x

TABLE 10: COMMON MEASURES WITH REGARD TO COMPLIANCE.

4.2 ADDITIONAL MEASURES SPECIFIC TO THE LOCAL CCN SUPPORT (LOCCCN)

4.2.1 SECURITY POLICY

None.

4.2.2 SECURITY ORGANIZATION

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
203	SecOrg	ISO must implement security at site level	Local Information Security Officers must institute programs at a site and/or departmental level to ensure that these CCN/CSI Security control objectives are implemented and followed (i.e. compliance program is initiated and maintained).	2	SM	1		x		x
210	SecOrg	Right to audit Third parties systems	Contractual agreements will grant CCN/CSI the right to audit the relevant systems within third parties and/or the third parties will commit to having independent, periodic audits performed which CCN/CSI will have the right to review.	2	SM	2		x		x

TABLE 11: ADDITIONAL MEASURES WITH REGARD TO SECURITY ORGANISATION (LOCCCN).

4.2.3 ASSET CLASSIFICATION AND CONTROL

None.

4.2.4 PERSONNEL SECURITY

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
401	PersoSec	Periodic review of access rights	Physical access to all CCN/CSI facilities must be controlled by the LSO with appropriate responsibility assigned for periodic inspection and review of security policies.	4	SM	1		x		x

TABLE 12: ADDITIONAL MEASURES WITH REGARD TO PERSONNEL SECURITY (LOCCCN).

4.2.5 PHYSICAL AND ENVIRONMENTAL SECURITY

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
501	PhysSec	Site security standards	Site physical security standards must meet the baseline requirements issued by CCN/TC Gateway Management Procedures (described in a separate document).	5	SM	1		x		x
502	PhysSec	Access to data centres	Access to data centres, computer rooms, labs, rooms containing wiring or communications equipment, and other restricted areas must be strictly controlled, monitored, and logged.	5	SM	1		x		x
507	PhysSec	UPS support	Uninterruptible power supplies (UPS) must be implemented, tested, and updated for power protection of servers and network equipment.	5	CI	1		x		x

TABLE 13: ADDITIONAL MEASURES WITH REGARD TO PHYSICAL AND ENVIRONMENTAL SECURITY (LOCCCN).

4.2.6 COMPUTER AND NETWORK OPERATIONS

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
602	ComNet Ops	NDCP virus checking	NDCP level virus checking must be done to ensure defence in depth (e.g., at Firewall, Mail server, etc.).	6	CI	1		x		x
603	ComNet Ops	Wireless LAN devices control	Wireless LAN products (e.g., NIC cards and access point devices) must not be attached to the CCN/CSI Network or to a device connected to the CCN/CSI Network without approval from CCN/CSI Security.	6	NW	1		x		x
604	ComNet Ops	Time sync across systems	A standardised time synchronization should occur across all equipment located inside the CCN DMZ and the EuroDomain to allow easy logfile consolidation.	6	CI	1		x		x
606	ComNet Ops	CCN/CSI Network must be secured from public and Third parties networks	Third-party connections (e.g. hardware suppliers maintenance modems) must be restricted to specific hosts, applications and files. Controls must ensure that a failure of logical security or any component of a third-party site/connection does not permit external users to gain access to unauthorized CCN/CSI resources.	6	NW	1		x		x
608	ComNet Ops	No Dial-in modems permanently connected on CCN/CSI Network	Modems (configured for dial-in) are not permitted on any device attached to CCN/CSI Network.	6	NW	1		x		x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
609	ComNet Ops	Traffic to entrusted networks must be filtered	Appropriate network separation must be ensured, traffic passing to and from entrusted networks must be filtered to control access (e.g. firewalls), and appropriate monitoring controls established to detect intrusions.	6	NW	1		x		x
610	ComNet Ops	IDS on critical segments	Network Intrusion Detection Systems (NIDS) must be installed on network segments where mission critical application systems reside unless a host-based IDS is installed on the server(s) where the critical application system is processed and where its data is stored.	6	NW	3		x		x
612	ComNet Ops	Internal IP addresses must stay hidden	The internal network-addressing scheme must not be visible via external connections (e.g. NAT usage).	6	NW	1		x		x
613	ComNet Ops	IP Spoofing protection	CCN/CSI networks must not accept connections from entrusted networks that appear to be originating from an internal CCN/CSI network address (i.e., to constrain IP address spoofing by using Ingress and Egress filtering).	6	NW	1		x		x
614	ComNet Ops	Changing default pwd on network devices	Default IDs and passwords for vendor system and/or network accounts should be changed during installation where feasible (e.g. network operating system, hubs, switches, routers, etc.).	6	NW	1		x		x
616	ComNet Ops	Monitoring of resources, services, and traffic	Adequate monitoring of CCN/CSI resources (processes, file systems, CPU, queues, etc.), services (synchronous, asynchronous, mail, intranet), and traffic (bandwidth usage) must be performed.	6	CI	1		x		x

TABLE 14: ADDITIONAL MEASURES WITH REGARD TO COMPUTER AND NETWORK OPERATIONS (LOCCCN).

4.2.7 SYSTEM ACCESS CONTROL

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
702	Access Ctrl	Keep register of access rights and approvers	Network access must be limited to authorised individuals on a need to do and/or know basis. At minimum, maintain a record of access approvers and of specific access granted to users.	7	CI	1		x		x
703	Access Ctrl	Access rights review when user function changes	Network & application access levels must be reassessed for appropriateness when job functions change (e.g. transfers) or during organizational changes (e.g., creation or merger of units, departments, etc.).	7	SM	1		x		x
705	Access Ctrl	Limit privileged account to those who need it	Limit privileged (e.g., command line, root, etc.) access to only those people who require it for their job function.	7	SM	1		x		x
706	Access Ctrl	Disable account after 90 days inactivity	Safeguards must be implemented to disable and/or revoke user account access after 90 days of inactivity	7	CI	1		x		x
707	Access Ctrl	User account disposal on leave	User accounts must be disabled upon termination/suspension of the user and user files are to be disposed of within 30 days after account termination.	7	CI	1		x		X
708	Access Ctrl	Pre-determined expiry of temporary accounts	Expire temporary accounts on a predetermined schedule (e.g. accounts for consultants)	7	CI	1		x		X
709	Access Ctrl	Network account lockout scheme	Network access accounts must be disabled after 10 login failures within one-hour duration. Disabled accounts must be reset manually.	7	CI	1		x		X

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
713	Access Ctrl	Unique user identification	UserIDs must uniquely identify users, and passwords must be maintained by the user and system as secret information. Other UserID and password guidelines include: UserIDs must not be shared by users. UserIDs used as server-level service accounts are exempt from this control; however, reasonable compensating security measures (e.g., such as strong passwords) should be implemented.	7	CI	1		x		X
714	Access Ctrl	CCN/CSI gateway must have unique identity	Each CCN/CSI gateway must have a unique identity. Any pair of gateways exchanging information between each other must authenticate themselves.	7	SM	1		x		x
717	Access Ctrl	Write access denied to public groups	Default user file permissions must not allow public groups (e.g. global, world, everyone, etc.) to have read and write access.	7	CI	2		x		x
728	Access Ctrl	Laptop access protection	Information and programs stored on portable computers and/or portable media must be adequately protected from modification and disclosure (e.g. encryption, digital signatures, etc.). Where encryption is not feasible, hard drive passwords/locks may be utilized. In those situations it is permissible for users to synchronize hard drive passwords with BIOS-type passwords and maintain them as non-expiring.	7	CI	2		x		x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
731	Access Ctrl	Procedure to report Access Token loss	Procedures and controls must be implemented to ensure the safekeeping of active authentication mechanisms (e.g., SecureID), including procedures to report loss of, disable, and/or reissue authentication mechanisms	7	CI	1		x		x
732	Access Ctrl	Procedure to supply Access devices replacements	Procedures must be implemented to issue temporary or permanent replacements using rigorous controls for verifying the identity of the requesting user (e.g. shared secret)	7	CI	1		x		x
735	Access Ctrl	Service account strong password (and/or expiration)	For service accounts (Tuxedo, LDAP), expiring passwords are preferred; however, if passwords are non-expiring, strong passwords must be implemented, including use of special characters, upper and lower case, and length of 8 to 15 characters.	7	CI	1		x		x
736	Access Ctrl	Service account periodic review	Service account owners (responsible of a service account) must perform annual and/or periodic reviews of account use and access to determine that the account is still required and that access continues to be properly restricted.	7	CI	1		x		x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
737	Access Ctrl	Event logs must be kept for at least 30 days	Logs of computer or communications system security relevant events must be created and securely retained for time periods specified by CCN/CSI General Security Policy, statutory, and/or business requirements. Business requirements and prevailing policy must be defined during early system design phases. A minimum of 30 days retention is required in support of incident investigation.	7	CI	1		x		x
739	Access Ctrl	Audit trails computer generated	Security measures must be designed and implemented for audit trails to be computer-generated.	7	CI	1		x		x
740	Access Ctrl	Audit trails secure from unauthorized modification	Security measures must be designed and implemented for audit trails to be secure from unauthorized modification.	7	CI	2		x		x
741	Access Ctrl	Audit trail on privileged accounts	Activities of privileged accounts must be logged and reviewed on a periodic basis.	7	CI	2		x		x
742	Access Ctrl	Audit trails on high risk scripts and batches	High risk/threat system processes, automated batch jobs, etc. must be logged.	7	CI	2		x		x
743	Access Ctrl	Audit trails on high risk system utilities	The execution of high risk/threat system utilities must be tracked.	7	CI	2		x		x
746	Access Ctrl	Mission Critical servers must alert on secevt	Mission critical servers must be protected by controls that detect and alert on security events.	7	CI	2		x		x
747	Access Ctrl	Record of system restarts	A record of operating system shutdowns and restarts must be maintained.	7	CI	1		x		x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
748	Access Ctrl	Audit trails date/time stamped	Procedures and controls must be designed and implemented for audit trails to be time- and date-stamped	7	CI	1		x		x
750	Access Ctrl	System Owner approval for Remote Access	All dial-in access and access via entrusted networks (e.g., ISPs, cable, application service providers, DSL connections, etc.), must use CCN/CSI approved access methods (e.g., Remote Access Server (RAS), SecureID, etc.)	7	SM	1		x		x
751	Access Ctrl	Justify need for Remote Access	Users must have a justifiable business case for remote access in order to be authorized for remote access by their management. Remote access includes all connections to CCN/CSI information or networks outside of CCN/CSI firewalls (e.g., ISPs, cable, application service providers, DSL connections, etc.).	7	SM	1		x		x
752	Access Ctrl	Remote Access Lockout after 10 attempts	Up to 10 remote access login attempts are permitted prior to lockout.	7	NW	1		x		x
753	Access Ctrl	Remote Access logon banners must be hidden	Remote access logon banners must not reveal information about the CCN/CSI system or network until successful authentication has occurred.	7	NW	1		x		x
754	Access Ctrl	Security on client when Remote Access is granted	PCs connected simultaneously to other networks (e.g. Internet or third party) and to CCN/CSI Networks or CCN/CSI information must have security against external intruders (e.g. Anti-virus, Anti-spyware).	7	NW	1		x		x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
755	Access Ctrl	Virus protection on client for Remote Access	Data files and programs must be protected from electronic attacks (e.g. viruses, Trojans, worms, etc.). CCN/CSI Security-approved anti-virus software must be implemented (excluding web-mail). Virus signature files must be updated daily on computers running operating systems and/or applications vulnerable to virus attacks (or upon connection to CCN/CSI Network and at other update frequencies deemed necessary by CCN/CSI Security).	7	CI	1		x		x
756	Access Ctrl	Sponsorship by CCN/TC employee for External's access	All non-CCN/CSI personnel who require access to CCN/CSI information resources must have sponsorship from an authorized CCN/CSI employee (e.g. hardware providers, auditors, consultants, visitors…).	7	SM	1		x		x
758	Access Ctrl	CA and Key recovery structures	Production use of cryptographic products requires that roles and responsibilities for centralized management and recovery of keys be implemented in a manner that ensures availability of Risk Level 2 and 3 information.	7	CI	2		x		x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
761	Access Ctrl	Systems hardening	Default operating system and application settings must be reviewed for security exposures, and steps must be taken to ensure identified vulnerabilities are addressed appropriately. At a minimum, unnecessary features, functions, services, etc., must be removed or disabled if possible, restrictive access control to sensitive privileges must be implemented, and trust relationships between systems must be restricted and supported by documented business requirements.	7	CI	2		x		x

TABLE 15: ADDITIONAL MEASURES WITH REGARD TO SYSTEM ACCESS CONTROL (LOCCCN).

4.2.8 SYSTEM DEVELOPMENT AND MAINTENANCE

None.

4.2.9 BUSINESS CONTINUITY PLANNING

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
908	BusiCont	Off-site archiving should be secured	CCN/CSI archived information (e.g. CCN/CSI source code) must be stored in a manner that prevents unauthorized disclosure. For example, archival vendors should demonstrate strong physical security capabilities and procedures.	9	CI	1		x		x
915	BusiCont	Fault tolerance of equipment	Subject to performance and cost considerations, the fault tolerance of components may be achieved by the implementation of: - Active dual encryption facilities; - Firewall fail over (e.g. based on the Virtual Router Redundancy Protocol); - Spare equipment available on site (router, hub, CCN gateway, LCMS).	9	CI	1		x		x

TABLE 16: ADDITIONAL MEASURES WITH REGARD TO BUSINESS CONTINUITY PLANNING (LOCCCN).

4.2.10 COMPLIANCE

None.

4.3 ADDITIONAL MEASURES SPECIFIC TO THE LOCAL APPLICATION SUPPORT (LOCAPP)

4.3.1 SECURITY POLICY

None.

4.3.2 SECURITY ORGANIZATION

None.

4.3.3 ASSET CLASSIFICATION AND CONTROL

None.

4.3.4 PERSONNEL SECURITY

None.

4.3.5 PHYSICAL AND ENVIRONMENTAL SECURITY

None.

4.3.6 COMPUTER AND NETWORK OPERATIONS

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
605	ComNet Ops	Limit concurrent connections	Concurrent network connections must be restricted (where applicable) except for authorized IT administrative accounts.	6	CI	3	x		x	
615	ComNet Ops	Controls for use of documentation	Adequate controls over the documentation for system operation and maintenance, must include periodic review and update to ensure accuracy.	6	CI	3	x		x	

TABLE 17: ADDITIONAL MEASURES WITH REGARD TO COMPUTER AND NETWORK OPERATIONS (LOCAPP).

4.3.7 SYSTEM ACCESS CONTROL

None.

4.3.8 SYSTEM DEVELOPMENT AND MAINTENANCE

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
801	SysDev&M	Security must be planned	CCN/CSI application development projects must define security requirements in the planning phase of system design. Control Requirements must be defined based upon a completed risk/threat assessment by business/information owners.	8	SD	2	x		x	
802	SysDev&M	Roles and responsibilities definition	The roles and responsibilities for individuals involved in the change control process (the process of controlling any change brought to the system, particularly software changes) must be clearly defined and properly segregated.	8	SD	2	x		x	x
803	SysDev&M	Unicity of source code	Only one live copy of source code should exist in the development environment to represent the production system or application.	8	SD	2	x		x	
808	SysDev&M	Emergency changes authorization	Information Owners must authorize all emergency changes to information resources (i.e. Risk Level 3 changes must be authorized before implementation; Risk Level 1 and 2 changes may be authorized and documented after-the-fact). For example CERT (Computer Emergency Response Team) alerts are to be implemented without delay. In these cases, documentation will be filled in “a posteriori”.	8	SD	1	x		x	x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
809	SysDev&M	Version tracking	Version control procedures must be documented and provide for an audit trail of changes to application software and its environment (e.g. source code versioning to avoid mix-up of older and newer versions).	8	SD	2	x		x	x
811	SysDev&M	Documentation of change requests	Change requests must be adequately documented via a change request process that includes approval from the defined application and/or system owner.	8	SD	2	x		x	x
812	SysDev&M	Restricted access to source code	Access to source code must be restricted to authorized programmers and their supervisors within the context of the change management process.	8	SD	2	x		x	x
813	SysDev&M	Test before install	All modifications, major enhancements, and new systems must be tested prior to installation of the software in production and receive implementation approval from the defined application and/or system owner.	8	SD	2	x		x	x
815	SysDev&M	Separate environments for development and production	Separate logical environments must exist for development, system configuration, system integration, and user acceptance testing and production source and production executable code.	8	SD	2	x		x	x

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
818	SysDev&M	Applications not able to use single sign-on must do as well as OS	Passwords must be of sufficient length and strength to deflect brute-force cracking attempts. At a minimum applications and operating systems that cannot interface with network authentication must meet the standards defined by measure 721. Those that cannot be configured to meet the above should use the maximum possible length and character complexity allowed by the OS or the application.	8	SD	2	x		x	
820	SysDev&M	Application inactivity timeout	Inactivity timeouts (generating log-offs when user is inactive) must be implemented based on risk.	8	SD	1	x		x	
888	SysDev&M	Application account lockout	Application user accounts must be disabled after 10 login failures occurring within one-hour duration. Disabled accounts must be reset manually.	8	SD	1	x		x	
889	SysDev&M	Client Applications authentication to the Gateway	Each CCN/CSI client application is connected using a unique identity. A user of a CCN/CSI client application can be a human user or a logical user. Generally, client applications on workstations are used by human users and server applications are used by logical users. Each user (human or logical) must have a unique identity in the National Domain. Any access by a client application to the CCN/CSI services must be identified and authenticated.	8	SM	1	x		x	

Id	Field	Security Measure	Description	ISO	ISF	Risk Level	Square Model Applicability			
							LocApp	LocCCN	CenlApp	CCN/TC
890	SysDev&M	Security services available as Generic Application Services (GAS)	If a new security measure is required by an application, and if that security measure is not specific to that application, i.e. that security measure is not particular to that application and may be required by other applications in the future, GAS will be the preferred way of implementing the new security service. For instance, if an application requires a non-repudiation mechanism, it should be implemented as a GAS because other applications might need the same service; but if an application requires application-level encryption for legal reasons, this specific encryption service should be implemented within the application.	8	SM	1	x		x	

TABLE 18: ADDITIONAL MEASURES WITH REGARD TO SYSTEM DEVELOPMENT AND MAINTENANCE (LOCAPP).

4.3.9 BUSINESS CONTINUITY PLANNING

None.

4.3.10 COMPLIANCE

None

END OF DOCUMENT