DOCUMENT XIII:

ACCREDITATION STRATEGY

FOR THE

FRAMEWORK AGREEMENT.

CLASSIFICATION LEVEL

RECORD OF CHANGES		
Date	*Issue*	*Changes*
20/07/2009	v. 2.0	Approved version
06/03/2008	v. 1.0	Approved version without annexes

INDEX:

1. INTRODUCTION:

The main objective of the Framework Agreement (also referred to as LoI) and the responsibility of its Subcommittee SC3 is to facilitate the access to the classified information required by Industry whilst maintaining an appropriate and adequate degree of security. The aim therefore is to facilitate support to defence industry involved in projects requiring classified data whilst ensuring that nations guarantee that the information provided is handled in a secure way.

So, with the aim of improving projects but also ensuring their security, it was agreed to develop a common strategy for the accreditation of IT systems in the context of the Framework Agreement. Under this strategy, national classified information, as released by nations, may be more easily exchanged when required.

The purpose of this paper is to define the terminology, the principles and the procedures for Framework Agreement nations to use during the accreditation of classified IT systems, which are to be used for projects with participants of more than one nation.

2. SECURITY PRINCIPLES:

As every country in the LoI community has its own laws and regulations for classified information, it is necessary to find a common frame of reference.

The Security Principles will be as follow:

- Only users with need to know and the appropriate clearance shall be allowed to access the System. They will be fully aware of their responsibilities when handling, transmitting or processing the classified information.

- The owner of the classified information shall clearly and formally state what the classified files are and their level and in what terms this information is provided.

- For the System to be accredited, a balanced set of security measures shall be defined. These measures include the following subjects:

    - Personnel Security.
    - Physical Security.
    - INFOSEC involving computing systems security, data separation, network security and cryptographic security.
    - EMSEC measures.
    - Disaster recovery procedures.
    - A process for incident response stating clearly what a security incident is and how to manage it.

3. PRINCIPLES OF LoI ACCREDITATION:

The principles of LoI Accreditation explain when an accreditation is needed and what type of Security Requirement Statement has to be completed for the accreditation process.

- A **National IT System** is an IT system, which is accredited and is operating in accordance with the regulations of the nation where it is located.

- A **LoI IT System** is an IT system for use by the participants in a Project which makes use of IT resources in different LoI nations.

- A **Separate LoI IT System** is a system in which there are no connections to any National IT System. A System Security Requirement Statement (SSRS) shall be written for each Separate LoI IT System. Connections between Separate LoI IT Systems are permitted, but each connection shall be accredited through a System Interconnection Security Requirement Statement (SISRS).

- Where a Project requires the interconnection of National Systems in more than one nation and the National Systems will continue to be accredited and operating in accordance with national regulations during the Project, the LoI IT System is defined as an **Interconnected LoI IT System**. A SISRS shall be written for each Interconnected LoI IT System.

- When the Project is a **National Programme** with participants in other LoI nations and the LoI IT System will handle classified information of only that nation, the national Security Accreditation Authority (SAA) of that nation shall be the sole accreditation authority for the LoI IT System. In such occurrences a Separate LoI IT System should normally be used, but the national SAA may permit the use of a national IT system with extensions into other nations. In this case, the national SAA will normally convene an Accreditation Panel with participation by the other nations involved.

- When the Project is a **Multinational Cooperative Programme**, so that the LoI IT System will be holding classified information owned by more than one nation, each participating nation will provide a member of its national SAA to a multinational Accreditation Panel.

4. ACCREDITATION AUTHORITIES AND ROLES:

To accomplish the Accreditation Process in a valuable and generally recognized way among the LoI countries, it is required to define the national participants and their roles. The participants will be the required authorities able to take decisions in an accreditation process. The involved Authorities will be known as ‘The Accreditation Panel’.

The Accreditation Panel will be composed of the national SAA responsible for the local accreditation of the System. The main idea is that every national SAA will be responsible for

its local components of the System and its branch of the network connection and the Panel should endorse the work of every national SAA and make a common agreement.

However, every national SAA must provide the Panel with the necessary information of its national part. This way, every country will be responsible for its national part of the system and the Panel for the whole System. In order to guarantee the maximum cooperation on this point, the local information on the System and Network configuration could be shared among the Panel members.

Apart from the Accreditation Panel, which is the head of the Accreditation Process for each LoI IT Systems two other roles shall be identified:

- **Operational Authority**. Organisation responsible for the System, able to take decisions related to the System Purpose and configuration. During development and manufacture, usually this role will lie with the Project Manager or Board of Managers if more than one. During the in-service life of the system, this role will lie with the owner of the system or with the System Manager. The members of the Operational Authority shall be appropriately cleared/authorised.

- **System Security Officer/Manager**. The member of the Operational Authority, who is responsible for the security of the IT System. Responsibilities include the writing and maintenance of system security requirement statements and of Security Operating Procedures (SecOPS), principal point of contact between the Operational Authority and the Accreditation Panel and maintenance of the secure configuration and operation of the IT system. He/She shall be invited to attend meetings of the Accreditation Panel.

5. CONSTITUTION OF THE ACCREDITATION PANEL

For a **Multinational Cooperative Programme**, the Accreditation Panel will elect a chairman from its members.

For a **national programme**, the Accreditation Panel, if convened, will confirm the representative of that nation as the chairman.

The Accreditation Panel may agree that the decisions of the chairman will be authoritative – this will be more likely for RESTRICTED IT systems – or may agree that decisions will be reached by mutual consent – this will be more likely for CONFIDENTIAL and above IT systems.

6. THE ACCREDITATION PROCESS.

Every time that a Multinational Cooperative Programme requires use of an IT System for the storage, processing and distribution of classified information belonging to any LoI country,

the national SAAs shall join and set up an Accreditation Panel to deal with the System Accreditation.

After the Panel is set up, every national SAA involved in this accreditation process will inspect and evaluate the System under its jurisdiction according to the stated Security Principles and Regulations, taking account of the SSRS/SISRS and SecOPS, and then give a positive or negative answer to the Accreditation Panel. Every national SAA giving a positive answer will make available to the Accreditation Panel the Document 'Statement of Compliance'.

The Panel will meet to consider every Statement of Compliance provided and approved. If approved by everyone, and there is no objection, the Panel will provide official approval by sending a formal letter to the NSA/DSA to be passed to the Operational Authority, by means of which will explain the terms of the Accreditation – Time, evaluations and conditions to follow.

7. ACCREDITATION PHASES.

Phase 1:

When a LoI IT System is required to handle classified information, the System shall be fully developed according to the appropriate Security Regulations. The System Security Configuration shall be reviewed by the System Security Officer/Manager. SecOPS, SSRS and SISRS, if appropriate, shall be sent to the Operational Authority of the System. The Operational Authority will add the general information of the System and will instruct the System Security Officer/Manager to send the whole set of documents to their national SAA for review, stating clearly that this is a LoI IT System. The Operational Authority will submit the Accreditation Plan to the relevant national SAA for approval.

Phase 2:

The national SAA shall inform the other national SAAs required for the Accreditation Process and will request the establishment of an Accreditation Panel. When it is satisfied, the Accreditation Panel shall endorse the set of documents provided in Phase 1 and shall notify this endorsement to the Operational Authority.

Phase 3:

When the Operational Authority has made appropriate progress in the development of the LoI IT System, the System Security Officer/Manager shall notify the Accreditation Panel. At the direction of the Accreditation Panel each national SAA will carry out its local inspection and evaluation and provide a Statement of Compliance. The LoI Accreditation Panel will consider all the Statements of Compliance for endorsement. If necessary, further details could be requested from the national SAAs.

Phase 4:

The Accreditation Panel will meet and determine whether the System can be accredited or not. If yes, the Accreditation Panel will send an Accreditation Certificate to the NSAs/DSAs of the nations participating in the LoI IT System for their relevant actions. If not, the Panel will highlight the deficiencies to be corrected. The Operational Authority shall correct these deficiencies and inform the Accreditation Panel who will review again the System.

Accreditation may fall into four different categories:

- Full accreditation – the system is fully approved for operation.
- Interim Approval to Operate (IATO) – an Interim Accreditation Certificate is designed to permit installation or testing or commissioning or an Initial Operating Capability, while security failings are being addressed. The period of validity of an Interim Certificate should be short, eg no longer than 6 months.
- Limited Approval to Operate (LATO) – where minor vulnerabilities are found or where the Operational Authority is prepared to accept risks, a Limited Approval Accreditation Certificate may be issued.
- Approval for Test (AfT) – where it is planned to submit a system to a long period of tests without handling classified information, an Approval for Test Accreditation Certificate may be issued.

The Accreditation Panel shall meet at least once in every phase from phase two of the accreditation process for IT Systems CONFIDENTIAL and above and at least once at phase four for RESTRICTED IT Systems.

8. POST ACCREDITATION TASKS.

1. Inspections

Every national SAA responsible for the local accreditation of the System will carry on inspections periodically to ensure that no changes have been made that may affect the overall security of the system and cause it not to be compliant anymore. If so, the national SAA will take appropriate actions at national level and report the situation to the Accreditation Panel which will inform the System Security Officer/Manager that the System is no longer authorised to handle classified information until the corrective security measures have been applied and a new inspection for verification has been performed.

2. System Modification

Prior to any modification of the System, which might affect the Security conditions of the System, the Operational Authority shall send a 'Modifications Proposal Document' to the

Accreditation Panel for consideration of the modification and, in case the security conditions are affected, the need for re-evaluation.

3. Reaccreditations

The Accreditation has a validity which is limited in time. Before expiration and if there is a need for reaccreditation, the Operational Authority shall initiate the reaccreditation process. Otherwise, a letter will be sent by the Accreditation Panel to the Operational Authority, with the statement that the system is no longer authorised to handle classified information.

ANNEX 1: DOCUMENTS OF REFERENCE

The following list shows the EU references that are of interest for systems accreditation.

2001/264/EC	Council's security regulations (dated 19 March 2001).
TECH-P-02-06	Policy on unencrypted distribution systems (UDS).
TECH-P-05	Policy on interconnections (draft).
PROC-P-01	Policy on accreditation.
PROC-P-06	Guidelines for the Development of Security Requirement Statements(EU ISP 201)
ISP202	Guidelines for the installation of sites and systems processing classified information.

ANNEX 2: LIST OF ACRONYMS

AfT	Approval for Testing
EU	European Union
IATO	Interim Approval To Operate
IT	Information Technology
LATO	Limited Approval To Operate
LoI	Letter of Intent
SAA	Security Accreditation Authority.
NSA/DSA	National Security Authority/Designated Security Authority
SecOPS	Security Operating Procedures
SISRS	System Interconnection Security Requirement Statement
SSRS	System Security Requirement Statement

ANNEX 3: GLOSSARY

Accreditation Panel	A group of representatives of the national SAA from each nation participating in a LoI IT system accreditation process.
Accreditation Plan	A document for each LoI IT System, which complies with this Accreditation Strategy and in which the timelines and milestones are coordinated with the overall plan for the implementation of the System.
Accreditation Strategy for the Framework Agreement	Document to describe in detail how the Accreditation Process works within the Framework Agreement.
Emsec	Emission Security. Part of the Security that tries to avoid or mitigate compromising electromagnetic emissions caused by electric and electronic devices.
Interconnection	Connection made between two systems in order to exchange information. The connection is made by defining Gateway A in System A and Gateway B in System B, and by making a network link between these two gateways. Communication is made between A and B only across Gateway A and Gateway B. In the network link will exist a number of network devices for routing and filtering the network traffic between these two gateways.
Interconnected LoI IT System	A LoI IT system that has connections to National IT Systems in more than one nation.
LoI IT System	An IT System for use by the participants in a Project which makes use of resources such as staff, equipment or information situated in different LoI nations
National IT System	An IT system, which is accredited and is operating in accordance with the regulations of one nation.
Operational Authority	Organisation responsible for the System, able to take decisions related to the System Purpose and configuration.

Policies	Generic Requirements to implement - and of course verify afterwards - within a system. For example: The existence of an Authentication Method, Use of Quality Passwords, Maximum Password Period, Auditing Controls, Open Network Ports Control, Event Logging and so on.
Security Accreditation Authority (SAA)	The Authority in each nation which is responsible for accreditation of classified IT systems. In some nations this responsibility may be delegated to an accreditation authority in another government department/organisation.
Security Operating Procedures (SecOPS)	The description of the implementation of the security measures, the security related operating procedures to be followed, and the personnel / user responsibilities.
Secure System	Set of computing hardware, software and network connections accredited for the storage, processing and distribution of classified information.
Security Regulations	Set of documents that provide the common Security Rules in the LoI framework to ensure that every accredited system is well designed in terms of security. The rules usually are packed according to the subject. For example, there might be rules for password quality, for user certificates for authentication, for event auditing and so on. The two first examples will be applicable for System Access and the last one for System Auditing. Regulations are generic and non-dependant on System Architecture.
Separate LoI IT system	An LoI IT system, which has no connections with any other IT system in any of the participating nations.
Statement of Compliance	Document provided by every National Security Authority to the LoI Accreditation Panel of the System. This document is usually a questionnaire with short answers type Yes/No, or short information. The Accreditation Panel will send a customized pattern document according to the Security Requirements regarding the System.

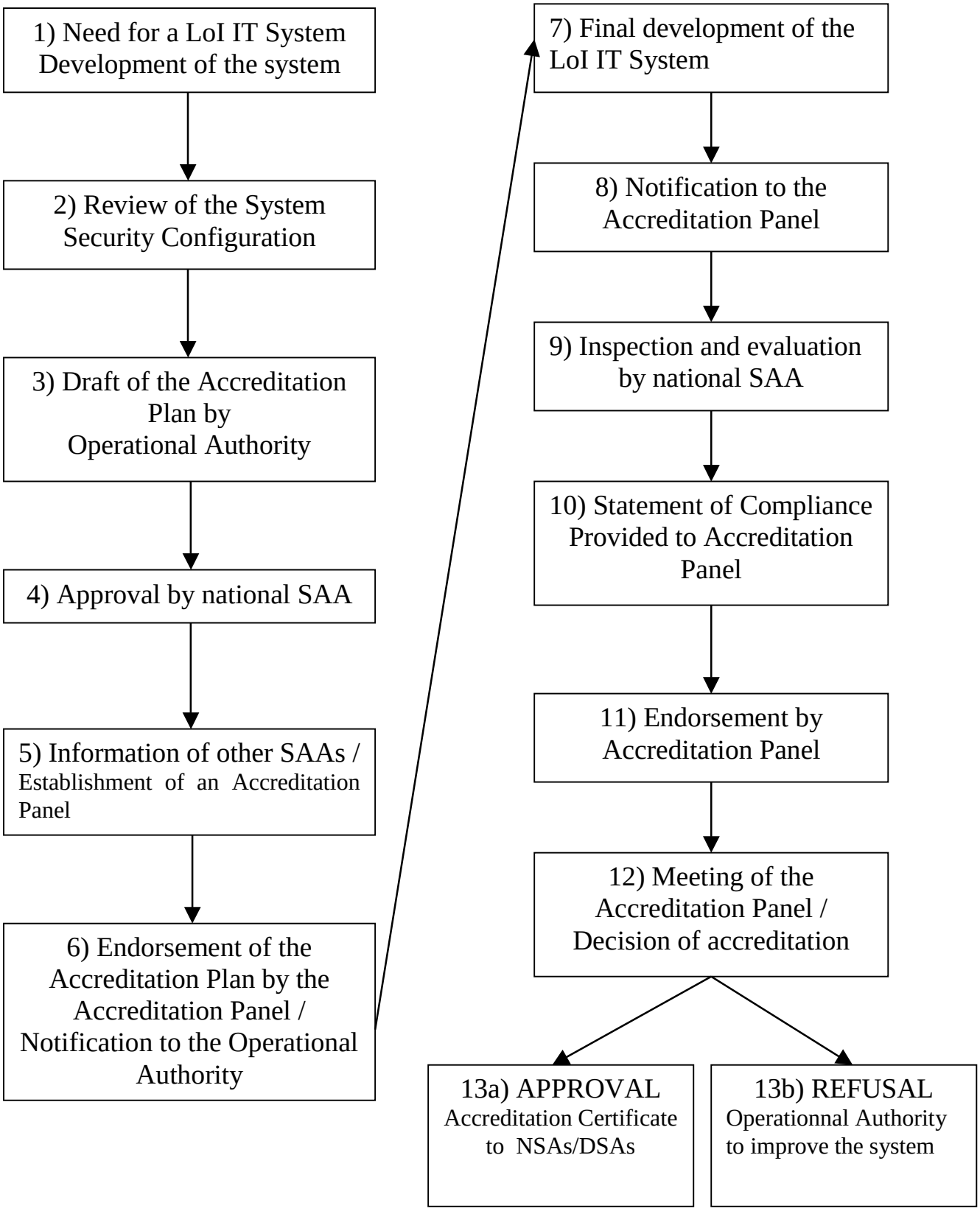
System Security Officer /Manager	The member of the Operational Authority, who is responsible for the security of the IT System.

ANNEX 4: GUIDANCE TABLE

Serial	System Type	System Location	Classified data	Operational Authority (OA)	System Security Officer/Manager / (SSO)	Security Accreditation Authority (SAA)	IT System Users	Accreditation process	Documents required	Who start the Accreditation Process
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
A	National IT System	Only one Nation	National	Project Manager/ System Manager	National Industry System Security Officer/Manager	National SAA	Nationally located	National	National accreditation documents	SSO to National SAA
B	LoI IT System	In more than one LoI Nation participating to the Project	In accordance with serials B1 to B4							
B1	Separate LoI IT System	It's a LoI IT system (ref. B) without any connection to national IT system	1.National. 2.Multinational	Project Manager (if there is one Nation leader) or Board of Project Managers	One member of the OA responsible for the security of the IT system	1. National SAA. 2. Accreditation Panel	Located in more than one Nation	LoI accreditation	Secops, SSRS, SOC	SSO to one National SAA (Same Nation of SSO)
B2	More than one Separate LoI IT System connected between them - Assume more than one Project, each	Each Separate LoI IT system is located over more than one Nation participating in	Multinational and/or National	Project Managers or Boards of Project Managers	One for each LoI IT system	Accreditation Panel formed by representatives of the SAAs for Serial B1	Located in more than one Nation	LoI accreditation	SISRS (plus documentation of already accreditated LoI IT systems)	SSO through SAA of each LoI IT System

	with its own LoI IT System	the Projects								
Serial	**System Type**	**System Location**	**Classified data**	**Operational Authority (OA)**	**System Security Officer/Manager / (SSO)**	**Security Accreditation Authority (SAA)**	**IT System Users**	**Accreditation process**	**Documents required**	**Who start the Accreditation Process**
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**	**(9)**	**(10)**	**(11)**
B3	Interconnected LoI IT System	More than one National IT System connected	Multinational	Project Manager (if there is one Nation leader) or Board of Project Managers	One member of the OA responsible for the security of the Interconnected IT System	Accreditation Panel (to be operational after National accreditations)	Located in more than one Nation	LoI accreditation (after national accreditations)	SISRS (plus national documentation of already accreditated national systems)	SSO to one National SAA (Same Nation of SSO)
B4	LoI IT System used for a National Programme with contractors in other LoI nations: a National IT System (Serial A) permitted by National SAA to be extended into other nations. (not a Separate LoI IT System (Serial B1).)	In any nation participating in the Project	National	Project Manager/ System Manager	One member of the OA responsible for the security of the IT system	An Accreditation Panel, if other nations require it. Otherwise, the National SAA.	Located in more than one Nation	LoI accreditation (after national accreditation)	1. Accreditation Panel: Secops, SSRS, SOC. 2. National SAA: national documentation, SOC.	SSO to National SAA

ANNEX 5: ACCREDITATION PROCESS



STEPS:

Step 1: Need for a LoI IT System to handle classified information. Development of the System according to the appropriate Security Regulations.

Step 2: Review of the System Security Configuration by the System Security Officer/Manager.
SecOPS, SSRS and SISRS, if appropriate, shall be sent to the Operational Authority of the System.

Step 3: The Operational Authority will add the general information of the System and will instruct the System Security Officer/Manager to send the whole set of documents to their national SAA for review, stating clearly that this is a LoI IT System.

Step 4: The Operational Authority will submit the Accreditation Plan to the relevant national SAA for approval.

Step 5: The national SAA shall inform the other national SAAs required for the Accreditation Process and will request the establishment of an Accreditation Panel.

Step 6: When it is satisfied, the Accreditation Panel shall endorse the set of documents provided in steps 3/4 and shall notify this endorsement to the Operational Authority.

Step 7: When the Operational Authority has made appropriate progress in the development of the LoI IT System, the System Security Officer/Manager shall notify the Accreditation Panel.

The LoI Accreditation Panel will consider all the Statements of Compliance for endorsement. If necessary, further details could be requested from the national SAAs.

Step 8: When the Operational Authority has made appropriate progress in the development of the LoI IT System, the System Security Officer/Manager shall notify the Accreditation Panel.

Step 9: Upon request of the Accreditation Panel each national SAA will carry out its local inspection and evaluation.

Step 10: Once step 9 achieved, each national SAA will provide a Statement of Compliance to the Accreditation Panel.

Step 11: The LoI Accreditation Panel will consider all the Statements of Compliance for endorsement. If necessary, further details could be requested from the national SAAs.

Step 12: The Accreditation Panel will meet and determine whether the System can be accredited or not.

Step 13:

13a) If the system is accredited, the Accreditation Panel will send an Accreditation Certificate to the NSAs/DSAs of the nations participating in the LoI IT System for their relevant actions.

13b) If the system is not accredited, the Panel will highlight the deficiencies to be corrected. The Operational Authority shall correct these deficiencies and inform the Accreditation Panel who will review again the System. The process will start again from step 7.

ANNEX 6: SYSTEM INTERCONNECTION SECURITY REQUIREMENT STATEMENT (SISRS)

In order to simplify proceedings, it has been agreed by all participating countries that Operational Authorities base their drafts of System Security Requirement Statements and of System Interconnection Security Requirement Statement (SISRS) on the Guidelines for the Development of Security Requirement Statements / PROC-P-06 (EU ISP 201) approved by the Council of the European Union.

Appendix 2 to this document gives guidance on the writing of a SSRS.
Appendix 3 to this document gives guidance on the writing of a SISRS.

In case, such document were updated or somehow modified Operating Authorities are requested to use the most updated version.

ANNEX 7: STATEMENT OF COMPLIANCE

Based on the state of security controls tested and evaluated during the inspection and evaluation of the elements of LoI IT system [name of the system] in [nation] at <[location1], [location 2], etc. >, this Security Accreditation Authority certifies that this system complies with the security requirements defined for IT systems handling Classification level Classified Information.

This Statement of Compliance is valid until [date], and is given as a [Full accreditation] [Interim Approval To Operate] [Limited Approval To Operate] [Approval for Test].

References of documentation presented:

DOCUMENT	REFERENCE
SSRS:	
SecOPS:	
SISRS:	
Security testing and evaluation report:	
Certificate of IT System accreditation:	

NSA/DSA	Name	Date	Stamp

ANNEX 8: CERTIFICATE OF SECURITY ACCREDITATION

COVER SHEET FOR TEMPLATE FOR CERTIFICATE OF SECURITY ACCREDITATION

1. This is the Cover sheet for the Template for the Certificate of Security Accreditation for the EDIR FA.

GUIDANCE FOR USE OF THE TEMPLATE

2. Use of the Template:

    a. Items in [ ] are required for each Certificate.
    b. Items in < > show choices to be made for [ ] items in each Certificate.
    c. For completion of the Certificate, delete all text in *Italics*.

3. Use of Sections:

    a. Choose to complete *Section A1*, *Section A2*, or *Section A3*, depending on the scope of the Certificate of Accreditation.
    b. Complete *Section B* only if relevant.
    c. Complete *Sections C, D and E* in all cases.

[reference]
[date]

FRAMEWORK AGREEMENT FOR EUROPEAN DEFENCE INDUSTRY RESTRUCTURING CERTIFICATE OF SECURITY ACCREDITATION FOR [NAME OF <LoI IT SYSTEM> <SYSTEM INTERCONNECTION> <INTERCONNECTED LoI IT SYSTEM>]

AUTHORITY

1. This Certificate of Security Accreditation is issued in accordance with the Framework Agreement Accreditation Strategy, which contains the definitions of all terms used in this certificate.

SECTION A1: <CERTIFICATE FOR A LoI IT SYSTEM>

2. The [name of LoI IT System] is a LoI IT system. The System Security Requirement Statement (SSRS), [reference, version and date], has been submitted by [name of Operating Authority].

3. The [name of LoI IT System] has been accredited by <name of national Security Accreditation Authority><an Accreditation Panel with members from [names of nations]> for operation at [security classification] for [period]. <This is a full accreditation and authority to operate.><This is an interim accreditation for operation for a limited period of [period].><This is a limited approval to operate.><This is an approval for test.> The Operating Authority is required to resubmit the SSRS for re-accreditation by [date].

SECTION A2: <CERTIFICATE FOR A SYSTEM INTERCONNECTION BETWEEN LoI IT SYSTEMS>

4. [name of LoI IT System] [name of LoI IT System] [name of LoI IT System] are LoI IT Systems. Their Operating Authorities have submitted the System Interconnection Security Requirement Statement (SISRS) [reference, version and date] for the accreditation of an interconnection between these LoI IT Systems, called [name of interconnection].

5. Certificates of Security Accreditation for LoI IT Systems. The LoI IT Systems to be interconnected under this SISRS are accredited for operation at [security classification] and their accreditations are shown in **Table 1**:

Serial	Name of LoI IT System	Reference and Date of Accreditation Certificate	Expiry of Accreditation Certificate
(a)	(b)	(c)	(d)
1	[name of LoI IT System]		
2	[name of LoI IT System]		
3	[name of LoI IT System]		

Table 1 - Accreditations of LoI IT Systems for this system interconnection.

6. The interconnection of [name of LoI IT System] [name of LoI IT System] [name of LoI IT System] by [name of Interconnection] has been accredited by <name of national Security Accreditation Authority><an Accreditation Panel with members from [names of nations]> for operation at [security classification]. <This is a full accreditation and authority to operate. If any of the LoI IT Systems in **Table 1** changes its security classification for operation or loses its accreditation, this accreditation certificate is automatically cancelled immediately. Otherwise, the Operating Authorities are required to re-submit the SISRS for re-accreditation by [date].><This is an interim accreditation for operation for a limited period of [period]. The Operating Authorities are required to resubmit the SISRS for re-accreditation by [date].><This is a limited approval to operate. If any of the LoI IT Systems in **Table 1** changes its security classification for operation or loses its accreditation, this accreditation certificate is automatically cancelled immediately. Otherwise, the Operating Authorities are required to re-submit the SISRS for re-accreditation by [date].><This is an approval for test. The Operating Authorities are required to resubmit the SISRS for re-accreditation by [date].>

SECTION A3: <CERTIFICATE FOR A LoI INTERCONNECTED IT SYSTEM>

7. [name of National IT System] [name of National IT System] [name of National IT System] are National IT Systems. Their Operating Authorities have submitted their System Security Requirement Statements, [references, versions and dates] and the System Interconnection Security Requirement Statement (SISRS) [reference, version and date] for the accreditation of [name of LoI Interconnected IT System]. The Operating Authority for [name of Interconnected LoI IT System] is [name of Operating Authority].

8. [name of LoI Interconnected IT System] has been accredited by an Accreditation Panel with members from [names of nations] for operation at [security classification]. <This is a full accreditation and authority to operate.><This is an interim accreditation for [period].> <This is a limited approval to operate.><This is an approval for test.> The Operating Authority is required to resubmit the SSRSs and SISRS for re-accreditation by [date].

SECTION B: REASONS FOR INTERIM ACCREDITATION, LIMITED APPROVAL TO OPERATE or APPROVAL FOR TEST (IF ANY)

9. Reason 1. etc

SECTION C: SIGNATURES OF ACCREDITATION AUTHORITIES

<[national Security Accreditation Authority]
Signature: Date:

<[national Security Accreditation Authority Chairman of Accreditation Panel]
Signature: Date:

[national Security Accreditation Authority]
Signature: Date:

[national Security Accreditation Authority]
Signature: Date:>

SECTION D: HISTORY OF PREVIOUS ACCREDITATION CERTIFICATES

10. Reference of Initial Accreditation: Date:
History:

11. Reference of Subsequent Accreditation: Date:
History:

SECTION E: STATEMENTS OF COMPLIANCE

12. During the Accreditation Process the following national Statements of Compliance were taken into account in the decision to accredit:

Serial	Nation Supplying Statement of Compliance	Reference and Date of Statement	Remarks and Recommendations
(a)	(b)	(c)	(d)
1			
2			
3			

Table 2 - Statements of Compliance.