NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

18 October 2010

DOCUMENT
AC/35-D/2005-REV2

NATO SECURITY COMMITTEE

INFOSEC MANAGEMENT DIRECTIVE for CIS

Note by the Chairman

1. At Annex 1 is the second revision of the "INFOSEC Management Directive for CIS". This document replaces AC/35-D/2005-REV1 which should be destroyed.

2. This directive is published by the NATO Security Committee in support of NATO Security Policy (C-M(2002)49), and the latest version of the Primary Directive on INFOSEC.

3. This directive has been approved by the NATO Security Committee under the silence procedure (AC/35-WP(2010)0009-AS1 refers), and will be subject to periodic review.

(Signed) Michael T. Evanoff

Annex : 1

Action officer: D.C. Murphy, NOS/POB, ext. 4592
Original: English

ANNEX 1
AC/35-D/2005-REV2

INFOSEC MANAGEMENT DIRECTIVE for CIS

TABLE OF CONTENTS

INTRODUCTION

1. This directive is applicable to security approval or accreditation authorities (for example, National Security Authorities (NSAs), and NATO Security Accreditation Authorities (SAAs)), CIS planning and implementation authorities, CIS operating authorities, security / system management staffs, project staffs, host nations, and procurement authorities responsible for establishing and implementing INFOSEC requirements, and for ensuring that INFOSEC measures are maintained.

2. This INFOSEC directive is mandatory and binding upon all CIS storing, processing or transmitting NATO classified information. Where required, specific guidance is published in support of this INFOSEC directive. This directive should be read in conjunction with NATO Security Policy, the Primary Directive on INFOSEC (published by the NSC and C3B), and the INFOSEC directives addressing INFOSEC technical and implementation aspects for CIS, published by the C3B.

3. This INFOSEC directive is published by the NATO Security Committee (NSC) in support of the NATO Information Management Policy (NIMP), the NATO policy for the protection of NATO classified information, and the Primary Directive on INFOSEC, and addresses the following aspects :

(a) Section I - INFOSEC Roles and Responsibilities;

(b) Section II - Security Approval or Accreditation of CIS;

(c) Section III - Security Risk Management for NATO CIS;

(d) Section IV - Security-related Documentation;

(e) Section V – "Pre-Approval" or “Pre-Accreditation” Security Implementation Verification;

(f) Section VI – "Post-Approval" or “Post-Accreditation” Security Inspection or Review of CIS;

(g) Section VII – Vulnerability Assessment of CIS;

(h) Section VIII – Security Approval or Accreditation of the Interconnection of NATO CIS; and

(i) Section IX - General INFOSEC Aspects.

SECTION I - INFOSEC ROLES and RESPONSIBILITIES

4. This section addresses the INFOSEC roles and responsibilities of authorities / personnel involved in the INFOSEC aspects of CIS.

I.1 Security Approval or Accreditation Authority(s)

5. The security approval or accreditation authority(s) is/are responsible for performing the following roles:

(a) providing advice and guidance on INFOSEC policy and directives (and supporting security measures) to civil and military bodies, CIS planning and implementation authorities, CIS operating authorities, security / system management staffs, project staffs, host nations, and procurement authorities;

(b) establishing a security approval or accreditation process, clearly stating the security approval or accreditation conditions for CIS under their authority. The security approval or accreditation processes may vary depending upon circumstances, but shall be subject always to NATO security policy and its supporting directives;

(c) reviewing and approving security-related documentation, for example, security risk management reports, Security Requirement Statements (SRSs), security implementation verification documentation (for example, security test and evaluation (ST&E) plans, and vulnerability assessment reports), and Security Operating Procedures (SecOPs), or national equivalent(s);

(d) reviewing additional documentation, for example, concepts of operation, system / product certification reports, trusted facility manuals, and security features user guides;

(e) providing a statement of security approval or accreditation for CIS, stating the conditions under which security re-approval or re-accreditation is required. Where a statement of "Interim Approval to Operate (IATO)" is provided, the statement shall identify the conditions to be applied to the interim approval and the activities required to achieve security approval or accreditation. Where a statement of “Limited Approval to Operate” is provided, the statement shall identify the changed operational environment and the limited duration period;

(f) checking the implementation of the security arrangements for the CIS under its responsibility, primarily by undertaking periodic security inspections or reviews in accordance with the security approval or accreditation process;

(g) liaising with CIS planning and implementation authorities, and CIS operating authorities in respect to security risk assessments, on-going security risk management, and the acceptance of residual risks;

(h) providing direction to the CIS planning and implementation authorities, CIS operating authorities and security / system management staffs in investigating any breach, or suspected breach, of the security arrangements, assessing the damage caused, providing advice / recommendations on corrective measures (or recommending sources for appropriate advice), and providing a report to the appropriate NATO military or civil authorities;

(i) advising the CIS planning and implementation authorities, and CIS operating authorities on the security risk and countermeasures implications of any proposed changes to the CIS;

(j) liaising with CIS operating authorities in respect to vulnerability assessments, the required level of vulnerability assessments, and the review of the results of the vulnerability assessments;

(k) liaising with other security approval or accreditation authorities in respect to interconnected CIS, for such purposes as agreeing System Interconnection Security Requirement Statements (SISRSs) or national equivalent(s);

(l) providing advice on the interconnection of NATO CIS to :

- NATO CIS in different security or management domains;
- National CIS;
- CIS associated with NATO co-operative efforts; or
- Internet or similar networks in the public domain;

(m) where a CIS is required to be evaluated and certified, liaising and co-ordinating with the appropriate National or NATO Evaluation and/or Certification Authority / Agency.

I.2 CIS Planning and Implementation Authority(s)

6. The CIS planning and implementation authority(s) is/are responsible for performing the following INFOSEC-related roles :

(a) establishing the INFOSEC technical and implementation aspects for CIS, in conjunction with the CIS operating authority(s) / project staffs, and the security approval or accreditation authority;

(b) providing advice and guidance on INFOSEC technical and implementation aspects of CIS to the security approval or accreditation authority;

(c) advising the CIS operating authority(s) of INFOSEC technical and implementation aspects of proposed changes to the CIS configuration, a change in its operational requirement or a change in the classification level of information being stored, processed or transmitted;

(d) providing the INFOSEC design requirements (for example, network and operating system security requirements, boundary protection component requirements, malicious software prevention requirements, and security management tools requirements, including intrusion detection / prevention systems) in operational requirements for CIS; and

(e) providing the INFOSEC resource requirements (for example, INFOSEC manpower requirements) in operational requirements for CIS.

I.3 CIS Operating Authority(s)

7. The CIS operating authority(s) is/are responsible for performing the following INFOSEC-related roles :

(a) formulating, and keeping under review, the security-related documentation required by the security approval or accreditation authority in respect to the CIS under its responsibility, and for interconnections to National / NATO CIS, to CIS associated with NATO co-operative efforts, or to Internet or similar networks in the public domain;

(b) providing proposals on the INFOSEC measures to be implemented, in close co-operation and consultation with the CIS planning and implementation authority(s) and the security approval or accreditation authority; and ensuring that the agreed INFOSEC measures are implemented;

(c) establishing, as early as possible in the CIS life-cycle, the resources required to fulfil day-to-day INFOSEC management functions;

(d) ensuring that arrangements are made for adequate and appropriate INFOSEC training;

(e) providing the required evidence to the security approval or accreditation authority in order that security approval or accreditation can be carried out in an effective manner, and requesting security re-approval or re-accreditation in accordance with the requirements of the security approval or accreditation process;

(f) operating and supporting the implemented INFOSEC measures in accordance with the conditions of the given security approval or accreditation;

(g) checking, periodically or in real-time, the implementation of INFOSEC measures to ensure that the security posture of the CIS is consistent with the requirements of the security approval or accreditation authority; and reporting to the security approval or accreditation authority in accordance with the requirements of the security approval or accreditation process; and

(h) investigating, in conjunction with the security approval or accreditation authority and the security / system management staffs, breaches, or

suspected breaches, of security within the CIS; assessing the damage caused and reporting the conclusions to the CIS planning and implementation authority(s) and the security approval or accreditation authority.

I.4 Security Management Staffs

8. The security management staffs are responsible for performing the following roles :

(a) formulating and maintaining Security Operating Procedures (SecOPs) (or national equivalent(s)) for the CIS, and circulating the SecOPs to system / network administrators and users on a periodic basis; and providing INFOSEC advice to, and maintaining INFOSEC awareness of, system / network administrators and users;

(b) maintaining a record of all persons authorised to use any part of the CIS and the extent of their authorisation; and ensuring that those persons have the appropriate security clearance and need-to-know for the information stored, processed, transmitted by the CIS;

(c) controlling and issuing passwords or other access control devices, ensuring that system / network administrators and users change their own passwords periodically;

(d) checking the implementation and maintenance of hardware, firmware and software modifications and enhancements to the CIS to ensure that security is maintained;

(e) ensuring the correct application of transmission, cryptographic, and emission security provisions, including the handling, maintenance and protection of cryptographic material, in accordance with the requirements of SDIP 293;

(f) ensuring the proper custody of classified computer storage media and other CIS machine- or human-readable documents; and carrying out spot checks and maintaining records of checks, at agreed intervals, on the presence of classified computer storage media and on the accuracy of their markings;

(g) ensuring that computer storage media to be released only contain that information authorised for release;

(h) ensuring that contractors or other organisations receiving classified computer storage media have the appropriate security provisions in place and need-to-know for the information, in accordance with the requirements of NATO Security Policy and its supporting directives;

(i) checking audit information for event / process failure, and unauthorised user and system activity;

(j) checking the back-up and recovery of system / network security relevant information;

(k) checking the configuration management aspects of changes to security-related hardware, firmware or software and associated documentation;

(l) reporting to the CIS operating authority and the appropriate security approval or accreditation authority any system / network security loopholes, infringements and vulnerabilities which may come to light; and

(m) ensuring the implementation and maintenance of the security provisions applicable to those areas of the site(s) hosting elements of the CIS.

I.5 Supporting Guidance

9. Supporting guidance published to identify the responsibilities of the authorities / personnel involved in the INFOSEC aspects of CIS should be consulted.

SECTION II - SECURITY APPROVAL OR ACCREDITATION OF CIS

II.1 Introduction

10. This section deals with the requirements for the security approval or accreditation of CIS. NATO security policy requires that all CIS storing, processing or transmitting NATO classified information shall be subject to a security approval or accreditation process. The security approval or accreditation requirements are as follows :

(a) for CIS storing, processing, or transmitting information classified NATO CONFIDENTIAL and above, security approval or accreditation shall be a structured process carried out by the security approval or accreditation authority, following either a process established by the security approval or accreditation authority or a process agreed for a specific CIS, and shall be subject to the requirements of this directive;

(b) for CIS storing, processing, or transmitting (at the highest) NATO RESTRICTED information, security approval or accreditation may not necessarily follow a structured process but shall reflect the importance of the security objectives (confidentiality, integrity and availability) and the aggregation of the impacts on the information and the supporting system services and resources. Security approval or accreditation may be delegated to an appropriate body according to local security regulations established by the security approval or accreditation authority (for example, NSA, Strategic Command (SC) Security Authority or the NATO Office of Security (NOS), or their delegated / nominated organisations or representatives (fulfilling the role of the security approval or accreditation authority)); and

(c) for the NATO CIS interconnection scenarios identified at paragraph 5(l) above, security approval or accreditation of the interconnection shall be subject to the requirements of this directive (see Section VIII).

II.2 General

11. The primary objective of security approval or accreditation is to ensure that the implemented CIS is conformant with NATO security policy and supporting directives, and the CIS-specific security-related documentation.

II.3 Pre-Approval or Pre-Accreditation Activities

The Bases for Security Approval or Accreditation

12. The primary bases for security approval or accreditation shall be the following :

(a) for NATO CIS, a review of the security risk assessment process and the resultant information;

(b) an assessment of the security-related documentation (for example, Security Risk Management Report, SRS(s), ST&E plans, and SecOPs (or national equivalent(s)));

(c) a verification that the security measures have been implemented (for example, review of the results of security testing, and security inspection), and are being maintained, in accordance with the security requirements; and

(d) for NATO CIS, an identification of the residual risk, and an identification of the ongoing security risk management processes.

Establishing a Security Approval or Accreditation Process

13. The security approval or accreditation authority shall establish a security approval or accreditation process for those CIS within its domain. The CIS planning and implementation authority(s) and CIS operating authority(s) of the CIS to be approved or accredited shall provide INFOSEC-related evidence to be used during the security approval or accreditation process. The security approval or accreditation process may vary depending upon circumstances, but shall always be subject to NATO security policy and supporting directives.

14. The security approval or accreditation process shall include the following aspects :

(a) the scope and purpose of the security approval or accreditation process, including National / NATO security policies to be followed;

(b) a broad description of the CIS, including interconnectivity requirements;

(c) the responsibilities of the authorities / personnel (for example, NATO / National security approval or accreditation authorities, CIS planning and implementation authority(s), CIS operating authority(s), and project staffs) involved in the security approval or accreditation process;

(d) the specific items of evidence that will be required, and the assessment process to be followed in order to reach a security approval or accreditation decision; and

(e) the processes for ensuring the continued security approval or accreditation of the CIS.

Security Approval or Accreditation Statement

15. After following the activities involved in reaching a security approval or accreditation decision, the security approval or accreditation authority has a number of options in respect of the statement of security approval or accreditation, as follows :

(a) security approval or accreditation - a statement of security approval or accreditation for a specified period of time for the originally intended operational environment, where no pre-specified conditions are to be met;

(b) security approval or accreditation for operation outside of the originally intended operational environment - for example, for a change in mission, to meet a crisis situation, or for more restrictive operations; or a “Limited Approval to Operate” for one-time limited duration scenarios;

(c) an "Interim Approval to Operate (IATO)" - identifying clearly stated pre-specified conditions for the "interim approval", the activities to be undertaken and completed prior to the granting of security approval or accreditation (for example, additional countermeasures to be implemented, or final approval of security-related documentation), and the timeframe for the "interim approval"; or

(d) disapproval - identifying specific deficiencies and recommended timeframe for corrective action.

II.4 Post-Approval or Post-Accreditation Activities

16. The security approval or accreditation authority shall continue to oversee the security arrangements for the CIS under its responsibility, primarily by carrying out periodic re-assessments of the security risks, and periodic inspections / reviews of the security arrangements in place, in accordance with the requirements of NATO security policy and supporting directives.

17. It is the responsibility of the CIS planning and implementation authority(s) / CIS operating authority(s) to inform the security approval or accreditation authority of, for example, any proposed changes to the CIS configuration, any change in its operational

requirement or any change in the classification level of information being stored, processed or transmitted. The security approval or accreditation authority shall advise on any security implications of any of the proposed changes. In this respect, the security re-approval or re-accreditation conditions shall be clearly stated in the security-related documentation for a CIS, or in a CIS-specific security approval or accreditation process.

18. Appendix 1 to this document shows the relationship between the INFOSEC-related activities of the NATO CIS life-cycle and the security approval or accreditation processes.

II.5 Supporting Guidance

19. Supporting guidance published to support the requirements for security approval or accreditation of CIS should be consulted.

SECTION III - SECURITY RISK MANAGEMENT FOR NATO CIS

III.1 Introduction

20. NATO policy requires that NATO CIS storing, processing or transmitting NATO information, in NATO civil and military bodies, be subject to security risk management. The principles of, and application of, security risk management may also be adopted by national security approval or accreditation authorities for national systems handling NATO information.

III.2 Definitions

21. For the purpose of this INFOSEC directive, the following definitions are used :

- *Security Risk* - the likelihood of a communication and information system's inherent vulnerability being exploited by the threats, leading to the system being compromised; and

- *Security Risk Management* - the total process of identifying, controlling and minimising uncertain events that may affect system resources.

III.3 General

22. Security risk assessment is the process of identifying security risks, i.e. the threats and vulnerabilities, of a CIS, determining their magnitude, and identifying areas needing safeguards or countermeasures. Security risk assessment serves to identify the risks that exist, identify the current security posture of the CIS in respect to storing, processing or transmitting information, and then assemble the information necessary for the selection of effective security countermeasures, based upon NATO security policy and supporting directives and guidance.

23. Security risk assessment contributes to the decision on which security measures shall be required, and how the apportionment between technical and alternative security

measures can be achieved, and gives an unbiased assessment of the residual risk. A benefit arising out of security risk assessment is the increased security awareness which will be apparent at all organisation levels, from top-level management to operations and ancillary staffs.

24. Security risk assessment is not a task which is accomplished once for all time. It shall be performed periodically, in accordance with the requirements of an agreed security approval or accreditation process, in order to keep up to date with changes to the threats and vulnerabilities; and to an organisation's mission, its information, facilities and equipment.

25. The major resources required for security risk assessment are time, skilled manpower, and, preferably, an automated security risk assessment tool using a sound methodology. For this reason, the first security risk assessment for a project or organisation will be the most resource intensive. Subsequent updates to a security risk assessment can be based on previous baselines of information, with a possible decrease in the time and resources required.

26. The time allowed to accomplish the security risk assessment should be commensurate with its objectives. A complex CIS with significant volumes of information, and large numbers of users, will require more resources than a smaller stand-alone information system with limited amounts of information and a small number of users.

27. The success of a security risk assessment depends, largely, on the role of top-level management in the process. There must be management agreement to the purpose and scope of the security risk assessment, with that support being expressed to all levels of the organisation; and management review and endorsement of the results of the security risk assessment.

28. Security risk management addresses the options for managing the risk, including reduction, transfer, elimination, avoidance and acceptance. The security risk may be reduced by implementing a managed system architecture which includes personnel security, physical security, security of information, and INFOSEC measures.

29. Security risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds, at optimal cost. It is also a collaborative process where representatives of various interest groups develop a shared understanding of requirements and options. Increased awareness will strengthen security and make it more compatible with user needs.

30. Security risk management for CIS presents some particular difficulties arising from the dynamic nature of risk factors and the rapid evolution of the technology. Failure to consider security risk factors in an adequate and timely manner may result in ineffective and unnecessarily costly security measures. Therefore, security risk management shall be considered as an integral part of the overall system life cycle process.

III.4 The Security Risk Assessment and Risk Management Processes

31. The security risk assessment process is a data collection and assessment exercise that addresses two basic questions:

(a) what assets are at risk; and

(b) what is the impact or consequence if the identified vulnerabilities are exploited successfully.

32. The security risk assessment and risk management processes shall be undertaken jointly by the NATO CIS planning and implementation authority(s) / NATO CIS operating authority(s) / project staffs and the NATO security approval or accreditation authority(s). The security risk assessment and risk management processes shall follow a structured approach (either carried out manually or using an automated tool), and shall include the following stages :

(a) identification of the scope and objective of the security risk assessment; the objective shall be agreed between the NATO CIS planning and implementation authority(s) / NATO CIS operating authority(s) / project staffs and the NATO security approval or accreditation authority(s);

(b) determination of the physical and information assets which contribute to the fulfilment of the mission of a NATO CIS, or an organisation's mission;

(c) determination of the value of the physical assets;

(d) determination of the value of the information assets against the following impacts: disclosure, modification, unavailability and destruction;

(e) identification of the threats and vulnerabilities to the risk environment, and the level of those threats and vulnerabilities;

(f) identification of existing countermeasures;

(g) determination of the necessary countermeasures and a comparison with existing measures; identifying those countermeasures which are already installed, and identifying those countermeasures which are recommended;

(h) review of the security risks and the recommended countermeasures, taking into account the following options, noting that NATO security policy requires that a minimum standard of protection be applied to NATO classified information :

- risk elimination – the objective being to totally eliminate the real or potential vulnerabilities, by implementing the countermeasures in full;

- physical and information asset loss prevention – the objective being to implement the countermeasures to prevent the loss as far as possible, knowing that some security risks cannot be eliminated due to technological or operational reasons;

- physical and information asset loss limitation – the objective being to implement countermeasures to the extent that the loss is limited to an acceptable level; or

- acceptance of the risk of physical and information asset loss – where a decision may be taken to accept the security risk and the consequences, for example, when the cost / impact of the loss is not significant, or the probability of loss is judged to be sufficiently small, or the cost of the countermeasures are much higher than, or not in balance with, the costs / impacts of the assessed losses; and

(i) development of a Security Risk Management Report, including the objective and scope of the security risk assessment, the value of the assets, a threat and vulnerability summary, a description of the countermeasures to be implemented, a description of the residual risk, and the processes for ongoing security risk management.

33. The outputs from the security risk management process can provide the details to be included in the security-related documentation required in the NATO security approval or accreditation process.

III.5 On-going Security Risk Management

34. After the completion of the initial security risk assessment process, the resultant baseline of information shall be retained and used as the basis for future updates. The requirement to conduct re-assessments shall be in accordance with the requirements of the NATO security approval or accreditation authority(s), or as stated in an agreed security approval or accreditation process.

III.6 Supporting Guidance

35. Supporting guidance published to support the principles of, and application of, security risk management should be consulted.

SECTION IV - SECURITY-RELATED DOCUMENTATION

36. This section deals with the security-related documentation requirements, in support of the security approval or accreditation process.

IV.1 Security Risk Management Report

37. Section III of this directive addresses security risk management for NATO CIS; and addresses the requirement for a Security Risk Management Report.

IV.2 Capability Packages (CPs) and Associated Documents

38. For NATO CIS, Capability Packages (CPs) and associated documents are developed on the basis of NATO operational requirements and are often utilised as a major part of the acquisition process. All NATO CIS CPs and associated documents shall address, coordinated by the appropriate planning, implementation, operating and security authorities, the required INFOSEC aspects.

IV.3 Security Requirement Statements (SRSs)

39. For all CIS storing, processing or transmitting information classified NATO CONFIDENTIAL and above, a Security Requirement Statement (SRS) (or national equivalent(s)) shall be required; to be formulated, or co-ordinated by the appropriate CIS planning authority / project staffs, and approved by the security approval or accreditation authority. Dependent upon the security approval or accreditation process of the security approval or accreditation authority, an SRS may be required for CIS storing, processing or transmitting (at the highest) NATO RESTRICTED information.

40. The SRS (or national equivalent(s)) shall be formulated at the earliest stage of a project's inception (i.e., in the CIS planning stage) and shall be developed and enhanced as the project develops, fulfilling different roles at different stages in the project and CIS life-cycle.

41. The SRS (or national equivalent(s)) is a complete and explicit statement of the security principles to be observed and of the detailed security requirements to be met. It is based on NATO security policy and supporting directives, and, for NATO CIS, the security risk management process, or imposed by parameters covering the operational environment such as the lowest level of personnel security clearance, the highest classification of information handled, the security mode of operation or user requirements. The SRS (or national equivalent(s)) forms an integral part of the user and operational requirement. In its final form, the SRS (or national equivalent(s)) constitutes a complete statement of what it means for the CIS to be secure.

42. In defining what it means for the CIS to be secure, the SRS (or national equivalent(s)) specifies how security is to be achieved, managed and checked. It forms the binding agreement between the CIS operating authority(s) and the security approval or accreditation authority, and constitutes part of the security approval or accreditation process. The SRS (or

national equivalent(s)) fulfils an important role in the security approval or accreditation process of the security approval or accreditation authority, or in a CIS-specific security approval or accreditation process.

43. The concept and practice of Evolutionary Acquisition (EA) adopted for NATO CIS means that the SRS (or national equivalent(s)) will often call for phased development and implementation of countermeasures. Security approval or accreditation will be similarly phased, reflecting incremental enhancement of security measures. However, it should be noted that EA can only be carried out in a rational and economic manner if the security requirements of the objective architecture are known and outlined.

44. If, for example, the security classification and / or the security environments of a CIS are expected to change in later phases of the EA, the implementation of enhanced security measures at that time can cause serious time-consuming and financial problems, unless they have been planned from the first phase.

Role of an SRS

45. The following outlines, in general terms, the role of the SRS (or national equivalent(s)) at the different stages in the CIS life-cycle. The stages identified are generic in nature and may be adapted to individual, NATO or National, procurement or acquisition methodologies :

(a) CIS planning – an SRS (or national equivalent(s)) shall initially be produced in outline form and address, in broad terms, each of the Security Environments applicable to the proposed project. This is then developed further during the project definition phase of a project, as a more detailed approach to the security requirements is formulated. When the CIS is to be designed to meet a specific requirement, the SRS (or national equivalent(s)), as agreed with the appropriate security approval or accreditation authority, forms the basic security input to the CIS development phase of the project;

(b) CIS development / procurement - during this stage, the technical content of the SRS (or national equivalent(s)) shall be enhanced to address the various security issues at a more detailed level. This would provide input to the overall CIS specification and, depending on the planned operational environment, may be developed into more specific statements;

(c) CIS implementation / security approval or accreditation - the SRS (or national equivalent(s)) shall form the basis for the formulation of Security Operating Procedures (SecOPs) (or national equivalent(s)), specifying the procedures that are to be implemented to secure the CIS. Before a CIS goes into live operation, the SRS (or national equivalent(s)), supported by the remaining evidence required by the security approval or accreditation process, shall form the basis for security approval or accreditation, by the appropriate security approval or accreditation authority. For projects where Evolutionary Acquisition is being followed, security approval or accreditation should take place when identified incremental phases have been completed;

(d) CIS operation / enhancement – the SRS (or national equivalent(s)) shall form the basis of an understanding between the CIS operating authority and the appropriate security approval or accreditation authority that the CIS is intended to operate in a secure manner. It defines the demarcation line between the security responsibilities devolved to the security / system management staffs and those resting with the appropriate security approval or accreditation authority, and other security staffs with jurisdiction in the same Global Security Environment / Local Security Environment. The SRS (or national equivalent(s)) is to be maintained under rigorous configuration control by the CIS operating authority over the CIS life-cycle and any changes made should be undertaken in conjunction with the security approval or accreditation authority. The SRS (or national equivalent(s)) is used as a reference point in security reviews / inspections and in any security re-approval or re-accreditation activities, for example, when enhancements are to be made or other proposals to change the configuration or operational use of the CIS are being considered; and

(e) CIS withdrawal from service / disposal of equipment - the SRS (or national equivalent(s)) shall provide the information required in respect to the actions to be undertaken, by the responsible authorities, at the withdrawal from service / disposal of equipment stage of the CIS.

Types of SRS

46. The SRS (or national equivalent(s)) may take one or more forms, dependent on the nature and complexity of the CIS. This directive identifies the use for each of the following statements :

(a) Community Security Requirement Statement (CSRS) – in situations where there is a community of interconnected CIS (a system of systems), a CSRS (or national equivalent(s)) shall be formulated. This is to be supported by individual SSRSs (or national equivalent(s)) for each of the interconnected CIS. In addition, this should facilitate the aggregation of a series of bilateral System Interconnection Security Requirement Statements (SISRSs) (or national equivalent(s)), and should set the security standards to be met by any other CIS wishing to join the community. Where the community involves a number of different CIS operating authorities and different security approval or accreditation authorities, the CSRS (or national equivalent(s)) review and approval processes may be undertaken by a number of co-ordinating security approval or accreditation authorities.

The CSRS (or national equivalent(s)) may also be used to cover a community of CIS in a large organisation (for example, NATO HQs, SCs, JFCs, CCs and NATO agencies), some of which may be interconnected, and where there are security environments (Global and / or Local) which are common to each CIS. In this situation, the CSRS (or national equivalent(s)) review and approval process shall be carried out by the organisation's security approval or accreditation authority;

(b) System-specific Security Requirement Statement (SSRS) - in elementary situations (for example, small stand-alone information systems), the only SRS (or national equivalent(s)) that may be required by the security approval or accreditation authority is an outline SSRS (or national equivalent(s)). In more complex cases (for example, large local area networks), where a more comprehensive statement is required, the SSRS (or national equivalent(s)) should evolve during the project life-cycle, and approved by the security approval or accreditation authority as part of the security approval or accreditation process;

(c) System Interconnection Security Requirement Statement (SISRS) – when two CIS are required to be interconnected to exchange information, an SISRS (or national equivalent(s)) is required to be formulated, which forms the basis of a security agreement between the two CIS operating authorities and the two security approval or accreditation authorities; and

(d) Security Target (or System-specific Electronic Information Security Requirement Statement (SEISRS)) - for CIS requiring evaluation and certification, the developers, the evaluators and the certifiers of the CIS require a more detailed statement of the technical aspects of the SSRS (or national equivalent(s)), in the form of a Security Target (or SEISRS), which should form the basis for certification, and be utilised in the security approval or accreditation process.

47. The types of SRSs (or national equivalent(s)) necessary in any given circumstance is determined by the security approval or accreditation authority, in conjunction with the CIS planning and implementation authority(s), CIS operating authority(s) or project staffs.

Security Test and Evaluation (ST&E) Plan

48. An ST&E Plan is a description of the security testing and, where appropriate, evaluation of the INFOSEC measures to be implemented. For each security-relevant or security-enforcing INFOSEC function, as determined by the security approval or accreditation authority, the following shall be identified for each security test :

(a) the objective of the security test;

(b) an outline description of the security test;

(c) a description of the execution of the security test; and

(d) the results of the security test.

49. The security test and evaluation requirements necessary in any given circumstance is determined by the security approval or accreditation authority, in conjunction with the CIS planning and implementation authority(s), CIS operating authority(s) or project staffs. The security approval or accreditation authority shall be responsible for approving the ST&E plan,

and the results of the security testing, as part of the security approval or accreditation process.

Security Operating Procedures (SecOPs)

50. SecOPs (or national equivalent(s)) are a description of the implementation of the security measures to be adopted, the operating procedures to be followed, and personnel responsibilities.

51. The SecOPs (or national equivalent(s)) shall be prepared by the CIS operating authority, in consultation with the CIS planning and implementation authority(s) and the security approval or accreditation authority, who shall co-ordinate with other security elements concerned. The security approval or accreditation authority shall approve the SecOPs (or national equivalent(s)), as part of the security approval or accreditation process, before authorising the storing, processing or transmitting of information classified NATO CONFIDENTIAL and above.

52. Dependent upon the security approval or accreditation process of a security approval or accreditation authority, SecOPs (or national equivalent(s)) may be required for CIS storing, processing or transmitting (at the highest) NATO RESTRICTED information, and for CIS with connections to public networks, for example, the Internet.

53. The following sections are required to be addressed in the SecOPs (or national equivalent(s)) :

(a) administration and organisation of security;

(b) personnel security, physical security, security of information;

(c) INFOSEC;

(d) emergency and contingency planning; and

(e) configuration management.

IV.4 Supporting Guidance

54. Supporting guidance published to support the security-related documentation requirements should be consulted including, where appropriate, "Common Criteria for IT Security Evaluation" guidance.

SECTION V - "Pre-APPROVAL" OR "Pre-ACCREDITATION" SECURITY IMPLEMENTATION VERIFICATION

55. This section addresses the requirements for security verification of the CIS to be implemented. The objectives of security implementation verification are the following :

(a) to verify that the personnel security, physical security, security of information, and INFOSEC controls are implemented as required (for example, through security inspection), and to identify any discrepancies;

(b) to verify, through appropriate security testing (based upon an agreed ST&E plan) that the INFOSEC features are implemented, and perform as specified and required, and to identify any discrepancies. In certain instances, the security approval or accreditation authority may require the INFOSEC features to be subject to technical evaluation and certification, based on NATO criteria (or Nationally / internationally approved equivalent); and

(c) to document the results of the security implementation verification, for input to the security approval or accreditation decision process.

56. The security approval or accreditation authority shall, in conjunction with the CIS planning and implementation authority(s) / CIS operating authority(s) / project staffs, establish the requirements for security implementation verification (for example, security testing and security inspection) for specific CIS implementations / interconnections, based upon the established security approval or accreditation process.

V.1 Evaluation and Certification

57. Evaluation is defined as the detailed technical examination, by or for the appropriate National or NATO Evaluation Authority / Agency or its nominated competent representatives, of the security aspects of a CIS or product. The evaluation confirms the presence of required security functionality, the absence of compromising side-effects from such functionality and makes an assessment of the incorruptibility of such functionality. The evaluation determines the extent to which the security requirements of a CIS, or the security claims for a product, are satisfied and establishes the assurance level of the CIS, or the product's trusted function.

58. The evaluation of a CIS or product is an independent examination to determine whether the CIS or product satisfies its pre-defined security requirements or security claims. Evaluation may therefore reveal faults in a CIS or product that result in these security requirements or claims not being fulfilled. In particular, as well as carrying out the technical examination, the aim of evaluation is to assemble evidence to allow the certifier to determine whether an implemented CIS or marketed product satisfies its functional security requirements or claims to the required assurance level.

59. Certification is defined as the issue, by an appropriate Authority / Agency of a formal statement, supported by an independent review of the conduct and results of an evaluation, of the extent to which :

(a) a CIS meets the INFOSEC requirement as specified in the SRS (or national equivalent(s)) and as agreed with the security approval or accreditation authority; or

(b) a product meets pre-defined security claims.

60. Certification is carried out by the certifiers, within the Certification Authority / Agency, once in receipt of the evaluation reports. It should be noted that the certifier maintains close contact with the evaluators throughout the evaluation. The certification process shall include the following aspects :

(a) resources for the evaluation - how much resource (for example, time or money) has been expended on the evaluation;

(b) personnel - who performed the evaluation, what were their qualifications, and might there be any reasons to question their objectivity;

(c) processes used in the evaluation - what technical review mechanisms were used, have the findings and recommendations been properly co-ordinated, what major tools and techniques were used, and have resources been effectively allocated to tools, analyses, and presentations of findings; and

(d) Evaluation Report - are the findings and recommendations reasonable, did the evaluation focus on those things of primary importance, what assurances are there that major problem areas have not been overlooked, are there safeguards not considered by the evaluation activity that might influence the findings, are the recommendations prioritised and what is the basis for the prioritisation, have any residual vulnerabilities been identified, and are the recommendations and judgements supported by quality information.

61. The certification process normally results in the production of certification reports which state to what extent the CIS or product meets the security requirements as defined in the SRS (or national equivalent(s)) or meets the security functionality claims as stated by the manufacturer of the product. In addition, the reports will also contain details of the conditions under which the certification remains valid.

62. Prior to security approval or accreditation, in certain instances (see paragraph 61), the multi-level secure (MLS) mode of operation shall require the INFOSEC features of a CIS to have been evaluated and certified, based on NATO criteria (or approved National / international criteria), as being capable of safeguarding information of mixed classification and information category designation, and of discriminating between users on the basis of their authorised access to the system. The requirements for evaluation and certification shall be identified in CIS planning, and clearly stated in the security-related documentation, as soon as the security mode of operation has been established.

63. The instances in the MLS mode of operation where evaluation and certification shall be required are as follows :

(a) CIS storing, processing or transmitting information classified COSMIC TOP SECRET, and / or Special Category information; and

(b) CIS storing, processing or transmitting information classified NATO SECRET, where the CIS is interconnected with another CIS.

64. In addition, irrespective of the security mode of operation, where CIS operating with different highest classification levels of information are interconnected and where the community of users lacks the security clearance for access to information on the higher-classified CIS (where the higher-classified CIS handles information classified NATO CONFIDENTIAL and/or above), then the mechanisms associated with the interconnection (protecting the higher-classified CIS) shall be subject to evaluation and certification.

65. For NATO CIS, irrespective of the security mode of operation and as a result of a security risk assessment, a NATO security approval or accreditation authority may determine that an evaluation and certification is required, or determine that periodic vulnerability assessments are required.

66. The evaluation and certification processes shall be carried out in accordance with approved guidelines by independent and impartial teams of technically qualified and appropriately cleared personnel acting on behalf of the appropriate security approval or accreditation authority. The security approval or accreditation authority shall be involved in the selection of the appropriate teams to carry out the evaluation and certification processes.

67. The teams may be provided from a Host Nation evaluation or certification authority or its nominated representatives, for example a competent and appropriately cleared contractor, or from the NAMILCOM Communications and Information Systems Security and Evaluation Agency (SECAN).

68. The evaluation and certification processes shall establish the extent to which the design and implementation of a particular CIS meets specified security requirements, as stated in the SRS (or national equivalent(s)). Relevant sections of the SRS (or national equivalent(s)) may require updating following evaluation and certification. The evaluation and certification processes should commence at the CIS specification stage and continue through the implementation stage.

69. The degree of the evaluation and certification effort may be lessened (for example, only involving integration aspects) where CIS are based on existing Nationally evaluated and certified INFOSEC products.

V.2 Supporting Guidance

70. Supporting guidance published to support the "pre-approval" or “pre-accreditation” security implementation verification requirements should be consulted.

SECTION VI - "Post-APPROVAL" OR "Post-ACCREDITATION" SECURITY INSPECTION or REVIEW OF CIS

71. This section deals with the requirements for the security inspection or review of CIS.

72. For all CIS storing, processing or transmitting information classified NATO CONFIDENTIAL and above, the CIS operating authority shall establish control procedures which shall ensure that all CIS changes are reviewed for their security implications. Regardless of classification, any CIS handling NATO classified information, which is connected to Internet or similar networks in the public domain, shall establish control procedures which shall ensure that all CIS changes are reviewed for their security implications.

73. The types of change that would give rise to security re-approval or re-accreditation, or that require the prior approval of the security approval or accreditation authority, shall be clearly identified and stated in the SRS (or national equivalent(s)).

74. All CIS storing, processing or transmitting information classified NATO CONFIDENTIAL and above shall be inspected or reviewed on a periodic basis by the security approval or accreditation authority. In respect of CIS storing, processing or transmitting COSMIC TOP SECRET or Special Category information, the inspections shall be carried out not less than once every 24 months. The objective of inspections is to ensure that the CIS continues to be conformant with NATO security policy and supporting directives, and the CIS-specific SRS(s) (or national equivalent(s)).

75. All CIS storing, processing or transmitting information classified NATO CONFIDENTIAL and above, and operating in the "system-high", "compartmented" or "multi-level secure (MLS)" security modes of operation, shall be subject to real-time security management through the use of appropriate security tools. The security tools to be utilised shall be subject to the approval of the security approval or accreditation authority, in conjunction with the CIS planning and implementation authority(s) and CIS operating authority(s), and shall have previously been assessed by an appropriate NATO / national organisation.

76. The security approval or accreditation authority shall establish the requirement, in conjunction with the CIS planning and implementation authority(s) and CIS operating authority(s), for the use of security tools to perform the following :

(a) identification of unauthorised activity;

(b) intrusion detection – where CIS are interconnected, or where CIS are connected to public networks;

(c) vulnerability assessment – where a security risk assessment has established that significant risks exist within the CIS's operating environment, and where required as identified in Section VII of this directive; and

(d) configuration checks – to ensure that the configuration is established and maintained in its approved or accredited state, in accordance with the requirements of the security-related documentation (for example, SRS (or national equivalent(s))).

77. The security approval or accreditation authority shall establish the requirement, in conjunction with the CIS planning and implementation authority(s) and CIS operating authority(s), for the reporting of security violations.

VI.1 Supporting Documentation

78. INFOSEC Management guidance and INFOSEC Technical and Implementation directives and guidance published to support the security inspection or review requirements, and the use of security tools should be consulted.

SECTION VII - VULNERABILITY ASSESSMENT OF CIS

VII.1 Introduction

79. A vulnerability assessment is a review of a CIS in order to ascertain its susceptibility to compromise of the security objectives – confidentiality, integrity or availability. A vulnerability assessment can determine the susceptibility of a CIS to a specific attack, or determine the opportunity to a threat agent to exploit a vulnerability(s). A vulnerability assessment can be undertaken either as part of an on-going security risk management process or as part of the on-going security approval or accreditation process.

VII.2 Types of Vulnerability Assessment

80. A macro-level vulnerability assessment is a documentation review addressing the operational services provided by the CIS and the overall CIS architecture. The CIS architecture is analysed to determine the set of potential access points for each adversary to attack and the paths that would lead to CIS assets.

81. A level 1 vulnerability assessment is the periodic security inspections or reviews carried out by the security approval or accreditation authority, resulting in the production of a formal report that is provided to the head of the organisation. The level 1 vulnerability assessment involves:

(a) the review of security-related documentation (for example, security requirement statements (SRSs) and security operating procedures (SecOPs) (or national equivalent(s));

(b) review of configuration management;

(c) interviews with management, security management staffs (for example, security officers, system and security administrators), and users; and

(d) site inspection of the personnel security, physical security, security of information, and INFOSEC measures in place.

82. A level 2 vulnerability assessment is carried out by the CIS operating authority (or by a competent NATO / National authority (for example, SECAN), in conjunction with the CIS operating authority). It should build upon the results of the level 1 vulnerability assessment, using security tools to map the CIS, test the system and network components for security weaknesses, and test the system management software for completeness. A report of the vulnerabilities is produced, together with recommendations to resolve them.

83. A level 3 or level 4 vulnerability assessment is carried out by an independent team (for example, a competent NATO / National authority (for example, SECAN)). These assessments should build upon the results of the level 1 and level 2 vulnerability assessments. The independent team actively attacks the CIS to exploit any weaknesses, using security tools (for example, network and host vulnerability scanners, network and host exploitation tools, and monitoring tools). Level 3 and Level 4 vulnerability assessments are carried out with the prior approval of the head of the organisation and the security approval or accreditation authority. Level 3 vulnerability assessments are carried out with, additionally, the full knowledge and close co-operation of the CIS operating authority (including system and security administrators).

VII.3 Requirements for Vulnerability Assessments

84. The security approval or accreditation authority shall, in conjunction with the head of the organisation and the CIS operating authority, determine the requirements for vulnerability assessments either as part of an on-going security risk management process or as part of the on-going security oversight, security approval or accreditation process. Where a requirement is established, the security approval or accreditation authority shall agree the mechanisms and procedures, and shall the review the results of the vulnerability assessment in order to determine whether additional security countermeasures are to be implemented. Level 2, level 3 and level 4 vulnerability assessments shall be subject to National and NATO legal requirements.

85. For all vulnerability assessments, the scope of the assessment shall be clearly established and documented. Where an independent, competent NATO or National authority is employed to fulfil the assessment, particular attention shall be given to the methodology and techniques used. Responsibilities and procedures shall also be clearly identified and documented.

86. For all vulnerability assessments, a report shall be produced indicating, as a minimum, the results of the assessment and any suggested countermeasures. The report shall be made available to the head of the organisation and the security approval or accreditation authority.

VII.4 Supporting Guidance

87. Supporting guidance published to support the vulnerability assessment requirements should be consulted.

SECTION VIII - SECURITY APPROVAL OR ACCREDITATION OF THE INTERCONNECTION OF NATO CIS

88. This section identifies and mandates the security approval or accreditation requirements for connecting NATO CIS to other CIS, including other NATO CIS, national CIS in NATO nations, CIS in non-NATO nations and international organisations, and the Internet or similar networks in the public domain.

89. The principles of security risk management, minimality, least privilege, self protecting node and defence-in-depth shall be applied when connecting NATO CIS to the other CIS identified in paragraph 86 above (reference. Primary Directive on INFOSEC).

90. The security approval or accreditation authority, in co-ordination with the appropriate CIS planning and implementation authority(s) / project staffs, CIS operating authority and security management staffs, shall :

(a) approve the method of interconnection, and the services provided;

(b) approve the security risk assessment and risk management methodology to be utilised; and agree the scope of the security risk assessment;

(c) review and approve the results of the security risk assessment, and approve the on-going security risk management processes;

(d) establish the requirement for security-related documentation;

(e) review and approve the required security-related documentation (for example, SISRS, or national equivalent(s));

(f) approve the mechanisms and/or procedures for ensuring the confidentiality of the information stored, processed or transmitted;

(g) approve the mechanisms and/or procedures for ensuring the integrity and/or availability of the information, and supporting system services and resources;

(h) approve the mechanisms and/or procedures required to meet the objectives of accountability;

(i) approve the mechanisms and/or procedures implemented to detect, react and recover from unauthorised and/or intruder activity; including the use of appropriate security tools;

(j) approve the mechanisms and/or procedures for ensuring that NATO classified information is not transmitted over unprotected communications;

(k) establish the requirements for security test and evaluation (ST&E), vulnerability assessment and inspection;

(l) approve the ST&E plan, to include, for NATO CIS storing, processing or transmitting NATO classified information, the degree and nature of penetration testing of the boundary protection mechanisms;

(m) review the results of security testing, vulnerability assessments, and inspections; and identify, where appropriate, any additional countermeasures to be implemented; and

(n) provide a security approval or accreditation statement for the interconnection; and state the conditions for security re-approval or re-accreditation, including the requirements for periodic security testing, vulnerability assessment and inspection.

VIII.1 Supporting Documentation

91. INFOSEC Technical and Implementation directives and guidance published to support the interconnection of CIS requirements should be consulted.

SECTION IX - GENERAL INFOSEC ASPECTS

IX.1 Handling and Control of Removable Computer Storage Media

92. All removable computer storage media holding NATO classified information are documents (reference. Glossary to NATO Security Policy) and shall bear an appropriate security classification marking. The overall security classification of an individual media item shall be at least as high as that of its most highly classified component. The security classification marking shall indicate the highest classification of information ever stored on the individual media item, unless downgraded according to approved procedures.

93. All removable computer storage media holding accountable information shall be controlled and handled in accordance with the requirements of NATO security policy and the supporting security of information directive. Where required by National rules and regulations, media holding information bearing additional classification markings may be considered as accountable information. The controls shall include, as a minimum :

(a) for COSMIC TOP SECRET and Special Category information, up-to-date records of the removable computer storage media shall be maintained within the Registry System. The removable computer storage media shall be subject to inventory, on an annual basis, and shall be periodically spot checked for their physical presence and contents (to ensure that an inappropriate Special Category is not stored on the media); and

(b) for NATO SECRET information, up-to-date records of the removable computer storage media shall be maintained within the Registry System, and periodic spot checks shall be conducted to verify the continued controls.

94. For NATO civil and military bodies, as part of security risk management, controls may be mandated by the security approval or accreditation authority for media holding information bearing additional classification markings.

IX.2 Downgrading, De-classification and Destruction of Computer Storage Media

95. NATO classified information electromagnetically or otherwise recorded on re-usable computer storage media, shall only be downgraded in accordance with procedures approved and stated in the security-related documentation.

96. When a computer storage medium comes to the end of its useful life, it should be de-classified whereupon it may be released and handled as unclassified. If the medium cannot be de-classified, it shall be destroyed by an approved procedure. Computer storage media which have held NATO SECRET, COSMIC TOP SECRET or Special Category information, for example ATOMAL and US-SIOP, may be destroyed but shall not be de-classified and released into the public domain.

IX.3 Security During Processing

97. In the case of CIS that have users not possessing a security clearance, the storing, processing and transmitting of information classified COSMIC TOP SECRET or Special Category information shall not be permitted.

98. Release of information classified NATO CONFIDENTIAL and above to unmanned facilities shall be prohibited unless special arrangements approved by the security approval or accreditation authority are in force, and have been specified in the security-related documentation.

IX.4 Security of Portable Computing Devices

99. Portable computing devices (for example, laptops, electronic notebooks and personal digital assistants (PDAs)) with fixed hard discs (or other non-volatile storage media), operating either in stand-alone mode or as networked configurations, are documents in the same sense as floppy diskettes, USB mass storage devices or other computer storage media.

100. These equipments shall be afforded the level of protection, in terms of access, handling, marking, accountability, storage and transportation, commensurate with the highest classification level of information ever stored or processed (until downgraded or de-classified in accordance with approved procedures); including the appropriate requirements for the encryption of the fixed and removable computer storage media.

IX.5 Use of Privately-Owned Equipment for Official NATO Work

101. The use of privately-owned removable computer storage media, software and hardware (for example, PCs and portable computing devices) with a storage capability shall be prohibited for storing, processing and transmitting information classified NATO

CONFIDENTIAL and above. For NATO RESTRICTED information, the appropriate NATO / National, Strategic Command (SC) or Agency regulations shall apply.

102. Privately-owned hardware, software and media shall only be brought into any Class I or Class II security area where NATO classified information is stored, processed or transmitted where authorised in accordance with the appropriate NATO / National, Strategic Command (SC) or Agency regulations.

IX.6 Use of Contractor-Owned or Nationally-Supplied Equipment for Official NATO Work

103. The use of contractor-owned equipment and software in organisations in support of official NATO work may be permitted by the Head of an organisation. The use of Nationally-provided equipment and software by employees in a NATO civil or military body may also be permitted; in this case, the equipment shall be brought under the control of the appropriate organisation's inventory. In either case, if the equipment is to be used for storing, processing or transmitting NATO classified information, then the appropriate security approval or accreditation authority shall be consulted in order that the security requirements that are applicable to the use of that equipment are properly considered and implemented.

APPENDIX 1
ANNEX 1
AC/35-D/2005-REV2

RELATIONSHIP BETWEEN THE INFOSEC-RELATED ACTIVITIES OF THE NATO CIS LIFE-CYCLE AND THE SECURITY APPROVAL OR ACCREDITATION PROCESSES

1. The following shows the relationship between the INFOSEC-related activities of the NATO CIS life-cycle and the security approval or accreditation processes.

CIS Life-Cycle Phase	NATO CIS Life-Cycle Processes	Security Approval or Accreditation Requirements	INFOSEC Products
CIS Planning	Establish user and security requirements	Initial security risk assessment	Manual or automated security risk assessment and risk management tools
	Capability Packages (CPs) and associated documents Definition Process	Initial security-related documentation	
CIS Development & Procurement	Type "B" Cost Estimate (TBCE) Definition Process Specification Development Process CIS Development CIS Procurement	Detailed security risk assessment Enhanced security-related documentation (for example, CSRS, SSRS, SISRS, Security Target) Establish security test and evaluation (ST&E) requirements and the ST&E Plan	Security requirements definition capture tools Common Criteria Protection Profile (PP) repository Functionality & assurance packages Security Targets
CIS Implementation & Security Approval or Accreditation	CIS Deployment - C3 System Implementation - Acceptance Testing - Completion of Project Documentation	Security risk management Security implementation verification Security approval or accreditation	INFOSEC products NATO Information Assurance Products Catalogue (NIAPC)

CIS Life-Cycle Phase	NATO CIS Life-Cycle Processes	Security Approval or Accreditation Requirements	INFOSEC Products
CIS Operation	CIS Operation	Security Operating Procedures (SecOPs) On-going security risk management Security inspection/review	Security tools
CIS Enhancement	Specification Development Process CIS Procurement CIS Deployment - C3 System Enhancement - Acceptance Testing	Security risk management Enhanced security-related documentation (for example, CSRS, SSRS, SISRS, Security Target, SecOPs) Establish security test and evaluation (ST&E) requirements and the ST&E Plan Security implementation verification Security re-approval or re-accreditation	Security requirements definition capture tools Common Criteria Protection Profile (PP) repository Functionality & assurance packages Security Targets INFOSEC products NATO Information Assurance Products Catalogue (NIAPC)
CIS Withdrawal from Service	Archiving / De-classification / Destruction of Media and Hard-Copy Disposal and Destruction of cryptoproducts and cryptosystems	Information required for Accountability purposes	