NATO UNCLASSIFIED

15 November 2013

DOCUMENT
AC/35-D/2004-REV3

SECURITY COMMITTEE

Primary Directive on CIS Security

Note by the Chairman

1. At Annex 1 is the third revision of the "Primary Directive on CIS Security".

2. This directive, approved by both SC in CIS Security format SC(CISS) and C3B under silence procedure, will be subject to periodic review.

3. The Primary Directive is published jointly by the Security Committee (SC) and the C3 Board (C3B) in support of NATO Security Policy (C-M(2002)49).

4. This document replaces AC/35-D/2004-REV2 which should be destroyed.

(Signed) Stephen F. Smith

1 Annex

Action officer: Mr. M. C[illegible] 45[illegible]

Primary Directive on Communication and Information System Security

Contents

1. Introduction

1.1. The requirement to protect NATO information, supporting system services and resources as well as supporting communication and information systems and other electronic systems (hereafter referred to CIS) is based upon the principles set out in the following policies:

(a) NATO Information Management Policy (NIMP) (C-M(2007)0118);

(b) Security within the North Atlantic Treaty Organisation (C-M(2002)49);

(c) NATO Policy on Cyber Defence (C-M(2011)0042).

1.2. In particular, Enclosure “B” of the Policy on Security within the North Atlantic Treaty Organisation defines Communication and Information System (CIS) Security as the application of security measures for the protection of CIS, and the information that is stored, processed or transmitted[1] in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

2. Purpose

2.1. The Primary Directive on CIS Security is published by the Security Committee (SC) and the Consultation, Command and Control Board (C3B), for the following purpose:

(a) to support the implementation of the NIMP, Enclosure "F" of the Policy on Security within the North Atlantic Treaty Organisation and the NATO Policy on Cyber Defence;

(b) to provide the relation among the NIMP, the Policy on Security within the North Atlantic Treaty Organisation, the NATO Policy on Cyber Defence, the CIS Security management directives and guidance published by the SC, and the CIS Security technical and implementation directives and guidance published by C3B;

(c) to set out the CIS Security activities in the life-cycle of CIS which are essential to identify an appropriate level of protection for CIS handling NATO information, cope with the evolving threat environment and enable organisations to fulfil their mission by aligning security with their business objectives;

(d) to identify NATO committees, NATO civil and military bodies, and National bodies with a responsibility on CIS Security.

[1] Hereafter referred to within this Directive as handled.

3. Scope

3.1. This Primary Directive is mandatory and binding upon CIS handling NATO classified information. It is supported by management and technical and implementation directives and guidance on CIS Security. In this directive, where it states “for NATO CIS”, it is only mandatory and binding upon CIS in NATO civil and military bodies and NATO CIS extended into national or multi-national bodies.

3.2. The Policy on Security within the North Atlantic Treaty Organisation and its Enclosure “F” on CIS Security are applicable exclusively to NATO classified information and supporting CIS while the NATO Information Management Policy and the NATO Policy on Cyber Defence require that appropriate protection is provided as well to NATO information and CIS other than classified.

3.3. As this Directive supports collectively the NATO Information Management Policy, the NATO Policy on Cyber Defence and the Policy on Security within the North Atlantic Treaty Organisation, it defines also CIS Security requirements for NATO Civil and Military Bodies to protect NATO CIS handling non-classified information.

3.4. National Security Authorities (NSAs), Designated Security Authorities (DSAs), Strategic Command Security Authorities, and the NATO Office of Security (NOS) are responsible for ensuring the implementation of this directive. The NATO CIS Security Accreditation Board (NSAB) shall ensure a consistent implementation of this directive for NATO CIS.

4. Security Objectives

4.1. Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation sets the following five security objectives:

(a) confidentiality - to ensure the confidentiality of information by controlling the disclosure of, and access to, NATO classified information, and supporting system services and resources;

(b) integrity - to ensure the integrity of NATO classified information, and supporting system services and resources;

(c) availability - to ensure the availability of NATO classified information, and supporting system services and resources;

(d) authentication - to ensure the reliable identification and authentication of persons, devices and services accessing CIS handling NATO classified information;

(e) non-repudiation - to ensure appropriate non-repudiation for individuals and entities having processed the information.

4.2. The degree of applicability of these security objectives is specific to any CIS and shall be determined by a number of factors including the mission objectives, the minimum security requirements established by the Policy on Security within the North Atlantic Treaty

Organisation and supporting Directives and, where appropriate, the results of the security risk management process.

5. Security Principles

5.1. In order to meet the security objectives the following security principles shall be followed:

(a) Security Risk Management - for NATO CIS, security risk management processes shall be applied throughout the lifecycle to monitor, reduce, eliminate, avoid or accept risks;

(b) Minimality - only the functions, protocols, and services required to carry out the operational mission shall be installed and used;

(c) Least Privilege – entities using CIS shall only be given privileges and authorisations they require to perform their tasks and duties;

(d) Self-protecting CIS - each CIS shall treat other CIS as un-trusted and implement protection measures to control the exchange of information with other CIS;

(e) Defence-in-Depth - protection measures shall be designed using an architectural approach and implemented in CIS components, in security products and in data to the extent possible, so that there are multiple lines of defence;

(f) Up-to-date Security Posture - secure configuration of CIS shall evolve to maintain the required level of security while addressing changes in the threat environment;

(g) Resilience - mission critical CIS shall have the ability to quickly adapt to and/or recover from any type of disruption in order to continue operations at an acceptable level based on the mission objectives and the security impact of the disruption;

(h) Security Functionality Assurance - the security functionality of mechanisms and products enabling or providing security services to CIS shall be assured by a qualified authority;

(i) Security Compliance - the application of these principles and the subsequent implementation of the protection measures shall be initially verified, continuously monitored, and periodically assessed by the SAA; results shall be reported to senior management commensurate with evolving risks and where deficiencies are identified, these shall be addressed.

6. Minimum security requirements

6.1. For CIS handling NATO information, there are minimum security requirements to be implemented in order that the security objectives are achieved. These minimum security requirements are set out in Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation, the Primary Directive on CIS Security and the directives and supporting documents on the management, technical and implementation aspects of CIS Security issued by SC and C3B.

6.2. For NATO CIS and other CIS handling NATO classified information[2], when not in contradiction with higher policies and directives, exceptional deviations from the minimum security requirements defined by SC and C3B in their Directives related to the management, technical and implementation aspects of CIS security shall only be authorised by SAAs or for NATO CIS handling non-classified information by designated NATO authorities. In both cases the following conditions apply:

(a) a formal security risk assessment is mandated to prove that mitigating measures have reduced the risk of not implementing the minimum security requirements to a level considered acceptable by the SAA or designated authority for non-classified CIS;

(b) the deviation from the minimum security requirements is positively assessed in the context of the overall security architecture which considers a balanced set of security measures to achieve an appropriate level of protection.

7. CIS Security controls

7.1. Security is dynamic in nature and shall be considered throughout the CIS life-cycle. Its requirements and effects shall be reviewed in each stage of the CIS life-cycle, from inception to disposal, through an iterative approach which allows deriving specific security measures from high level security controls of policy, organisational, procedural and technical nature.

7.2. Security is an enabler of an organization's requirements for secure, reliable information-sharing, even though it may constrain the solutions that can be implemented. It has an impact on the associated civil works, the organisation of the operation and maintenance, on personnel requirements and costs. Security planning shall therefore involve the close interaction between the operational user, CIS planning and implementation authorities (CISPIA) (e.g. system architects), CIS Providers (CISP) and the appropriate SAAs.

7.3. In order to counter threats and reduce or eliminate vulnerabilities, security shall be addressed at project inception, starting from the conception of the CIS, so that cost-effective countermeasures can be provided to minimize the security risks anticipated during the development and operation phases of the CIS life-cycle. Countermeasures introduced retrospectively will inevitably be more expensive, and may well be less effective, than those identified and addressed at the inception of the project. Nevertheless, just as security risks evolve, based on changing CIS value, threats and vulnerabilities, so too do countermeasures evolve. CIS planners therefore shall ensure that sufficient funding and resources are available and allocated for the security aspects of the CIS, at all stages. CIS planners shall also ensure that the requirements for products related to CIS Security are clearly identified.

[2] In this Directive the description "NATO CIS and other CIS handling NATO classified information" refers to all NATO CIS including those handling non-classified information.

7.4. In order to guarantee that NATO information and CIS are protected by a balanced set of security measures in a cost-effective manner, CIS Security policies, processes, roles and measures shall be designed and managed to mutually complement and integrate with those related to personnel security, physical security, security of information and, where appropriate, industrial security.

7.5. CIS Security Policy Governance

7.5.1. Governing CIS Security includes establishing strategic direction, through policies, directives and guidance on the protection of CIS handling NATO information, as well as defining related roles and responsibilities. In this context, the following authorities are identified:

(a) the SC responsible for the Enclosure “F” (CIS Security) of the Policy on Security within the North Atlantic Treaty Organisation;

(b) the SC in CIS Security Format (SC(CISS)), responsible for the Primary Directive on CIS Security as well as for directives, supporting documents and guidance on the management aspects of CIS Security;

(c) the C3B and its substructure, responsible for directives, supporting documents and guidance on the technical and implementation aspects of CIS Security;

(d) the Defence Policy and Planning Committee in reinforced format (DPPC(R)), responsible for the Cyber Defence Policy;

(e) the Military Committee (NAMILCOM) for military requirements;

(f) various NATO civil committees for their civil requirements.

7.5.2. Additional NATO and national bodies directly or indirectly involved in CIS Security matters are listed at Annex I.

7.6. Risk management

7.6.1. Security risk management is a systematic approach to determine which security counter-measures are required to protect information and CIS, based upon an assessment of the assets value, threats, vulnerabilities and impact on the mission objectives. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.

7.6.2. Security risk management processes shall be applied to monitor, reduce, eliminate, avoid or accept risks associated with NATO CIS. The aim is to select a solution which results in a satisfactory trade-off between user requirements, resources and residual security risk whilst ensuring that minimum security requirements are applied for the protection of NATO information, in accordance with the requirements of NATO security policies and supporting directives.

7.6.3. For NATO CIS, security risk assessment, as part of security risk management, shall be embedded in the system development process. It is conducted jointly by representatives of the CIS Operational Authority (CISOA), CISPIA, CISP and SAA or designated NATO authority for non-classified CIS, using an agreed security risk assessment methodology. It involves assessment of existing, enhanced or new options, including balanced sets of technical and non-technical security measures.

7.6.4. The residual security risk is the risk which remains after implementing the security measures in a CIS, based on the understanding that not all threats can be countered and not all vulnerabilities can be eliminated or reduced. Threats and vulnerabilities are dynamic, therefore the residual risk changes. For this reason, risk shall be managed throughout the life-cycle of NATO CIS, implying that resources will be required to address security risk management through, by example, maintaining secure configuration baselines, analyzing the security impact of system changes, and reporting security compliance.

7.6.5. **Threats and vulnerabilities**

7.6.5.1. The security risk assessment shall be based on a current and up-to-date threat assessment and address the impact of threats and vulnerabilities on the achievement of the security objectives. A threat may be defined, in general terms, as the potential for the accidental or deliberate compromise of security. In the case of CIS Security, such a compromise involves loss of one or more of the security objectives of CIS Security.

7.6.5.2. A vulnerability may be defined as a weakness or lack of controls that would allow or facilitate a threat actuation against a specific asset or target. A vulnerability may be an omission or it may relate to a deficiency in a control's strength, completeness or consistency and may be technical, procedural or operational in nature.

7.6.5.3. Within NATO, there are a significant number of CIS handling NATO information, ranging from stand-alone computers and mobile devices, through small Local Area Networks (LANs), to large and complex Wide Area Networks (WANs). NATO information, in a concentrated form designed for rapid retrieval, communication and use, may be vulnerable to access by unauthorised users, to denial of access to authorised users, and to corruption, unauthorised modification and unauthorised deletion. Furthermore, the complex and sometimes fragile system equipment is expensive and often difficult to repair or replace rapidly.

7.6.5.4. CIS are attractive targets for intelligence gathering operations, especially if security measures are ineffective. They can enable large quantities of NATO information to be obtained quickly and surreptitiously. Any operation carried out by hostile intelligence services (or subversive organisation's and terrorist group's members or sympathisers) targeting NATO and its member nations is likely to be well planned and executed. Denial of authorised access to CIS or corruption of the data within them may be an equally attractive target, and no less harmful to NATO's missions, whether or not the information involved is classified.

7.6.5.5. The insider represents a unique threat vector to any organisation because of its privileged position in respect to physical and logical access to its CIS and the information within them. In contrast to an outsider, an insider has better situational awareness (e.g. knowledge of weaknesses), more time, fewer security controls to bypass and legitimate privileges for access to secure areas, CIS and information, by virtue of his/her role within the organisation (e.g. system administrator). These factors, combined with the possibility for an insider to commit any type of malicious act, would certainly magnify the impact of any incident.

7.6.5.6. Therefore, in order to deter, prevent and counter such a particular threat a set of specific security measures, shall be applied to CIS handling NATO information. In the selection of these measures, organisations shall take into account also the following:

(a) security measures shall be specifically designed to cope with the insider threat and support incident response and investigative procedures;

(b) close coordination and information sharing among the internal or external organisational elements (e.g. Personnel Security, Physical Security, Human Resources, Intelligence) which can contribute managing properly the insider threat shall be established.

7.7. Security Accreditation

7.7.1. The security accreditation process shall determine the extent to which CIS Security measures are to be relied upon for the protection of NATO information and CIS, during the process of establishing the security requirements.

7.7.2. The security accreditation process shall determine that an adequate level of protection has been achieved and is being maintained. Central to this process is the identification of an acceptable level of residual risk which needs to be monitored throughout the CIS life-cycle.

7.7.3. The security accreditation process shall be carried out for NATO CIS and other CIS handling NATO classified information, in accordance with the requirements of the relevant CIS Security management directives.

7.7.4. The responsibility for the security accreditation process is assigned to:

(a) SAAs for CIS handling NATO classified information and non-classified NATO CIS providing services essential to achieve the security objectives of NATO classified CIS (e.g. non-classified network providing bearer service to classified CIS);

(b) Heads of NATO Civil and Military Bodies for NATO CIS handling only non-classified information.

7.7.5. Security accreditation of NATO CIS handling non-classified information may involve the SAA as a result of a joint decision between the Head of a NATO Body and the relevant SAA, considering aspects such as the criticality and sensitivity of the CIS,

the overall impact that a compromise of the security objectives would have, the need for a more independent and thorough approach to security accreditation and resource implications.

7.7.6. Where the involvement of the SAA is deemed necessary, this shall be formalised in the Security Accreditation Plan (SAP) which shall be approved by both the Head of the NATO Body and the relevant SAA.

7.7.7. For NATO CIS handling non-classified information, the SAA retains authority to verify that these CIS are built and maintained conformant to the relevant NATO policies, directives and supporting documents addressing CIS Security.

7.7.8. Where a NATO CIS handling non-classified information falls under the responsibility of more than one NATO Body, a joint security accreditation board shall be established or identified, following advice by the NSAB.

7.7.9. Security-related documentation shall be established and maintained in accordance with the requirements of the relevant CIS Security management directives and the SAA. Security-related documentation shall be required throughout the CIS life-cycle, from the planning stage until the disposal stage. The security-related documentation shall be developed in an iterative process throughout the CIS life-cycle.

7.8. **Security audit**

7.8.1. Security audits shall be performed to verify that NATO CIS and other CIS handling NATO classified information comply with NATO policies, directives and supporting documents on CIS Security, and operate in accordance to the security baselines defined by the CISP, in conjunction with the SAA or designated authority for NATO CIS handling non-classified information. Security audits may also be used to support prevention or investigation of incidents.

7.8.2. Security audit methods include security inspections, reviews, interviews and tests. Whenever possible, reviews and tests shall be supported by automated tools.

7.8.3. Security audits shall be conducted in accordance with the requirements set in the appropriate directives on the management aspects of CIS Security and under the authority of the SAA.

7.8.4. For NATO CIS, security audits shall be carried out as well to:

(a) verify that the security measures, resultant from the security risk management process, are correctly implemented and maintained;

(b) validate the appropriateness of the security risk management process and results;

(c) verify that security standards (e.g. security baselines, security architectures) are consistently adopted throughout NATO;

(d) assess the maturity of CIS Security capabilities and the status of implementation of related programmes/projects;

(e) assess the effectiveness of CIS Security processes and capabilities by means of measures and measurement.

7.9. Business continuity

7.9.1. Business continuity is a key process that identifies potential impacts threatening an organisation's mission. It also provides a framework for building resilience with the capability for an effective response that minimises disruption to the organisation and its mission objectives in the event of an incident.

7.9.2. In the context of business continuity, the security measures necessary to support resilience in a NATO CIS, including plans and procedures, shall be identified through security risk assessment and business impact analysis and formalised in the context of the overall Business Continuity Plan (BCP) of an organisation. While the security risk assessment shall identify the critical functions and assets and the risks that can cause interruptions to the organisation's mission, a business impact analysis shall be undertaken to identify the potential damage or loss in the event of an incident, the form that the damage may take and how the degree of damage may increase over time.

7.10. Trustworthiness management

7.10.1. Trustworthiness in CIS Security is a complex issue that regards CIS, their components and the supply chain through which these are acquired as well as other parties that may have an impact on CIS Security. Managing trustworthiness is a key element as this allows determining the extent to which CIS, their components and related supply chains are to be relied upon for the protection of NATO information and supporting CIS. Evidence of trustworthiness can be produced using specific and formal assurance techniques, such as certification of products or vendors' processes, or less rigorous means such as information about the manufacturer (e.g. reputation).

7.10.2. Security functionalities of NATO CIS and national CIS handling NATO classified information and related products shall be assured by trusted authorities through formal assurance techniques.

7.10.3. Formal assurance techniques for products include:

(a) Evaluation as the detailed technical examination, by the appropriate national, international or NATO evaluation authority, of the security aspects of a 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 claims for a product are satisfied and establishes the conformance of the product's trusted function.

(b) Certification as the issue, by an appropriate national, international or NATO evaluation authority, of a formal statement, as a result of a successful evaluation as described above;

(c) Approval as the issue, by an appropriate authority, of a formal statement, supported by an independent review of the conduct and results of an evaluation and/or a certification, approving the use of a product for a specific purpose and under specific conditions.

7.10.4. Formal assurance techniques for CIS include:

(a) Evaluation as the independent examination, by the appropriate national or NATO authority, of the security aspects of a CIS. The evaluation determines whether the CIS satisfies its pre-defined security requirements;

(b) Security accreditation as the process which, supported by the results of an evaluation, determines that an adequate level of protection has been achieved and is being maintained for a CIS.

7.10.5. Assurance requirements for NATO CIS and other CIS handling NATO classified information shall be identified in the CIS Planning phase by the CISPIA, in conjunction with the SAA or designated NATO authority for NATO CIS handling non-classified information. This shall take into account the requirements set in the Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation and supporting Directives, and, where applicable, an assessment of the security architecture and the outcome of the security risk management process.

7.10.6. Assurance requirements for cryptographic products or mechanisms shall be in accordance with the provisions of Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation and relevant technical and implementation directives and supporting documents on CIS Security.

7.10.7. When evaluation and certification of products are required, the Common Criteria methodology (or national or international equivalent) shall, where appropriate[3], be used.

7.10.8. The use of security-enforcing hardware, firmware and software[4], which has been subject to a detailed design specification, should be limited to that designed and manufactured in NATO member nation(s). Where these are designed and/or manufactured in a non-NATO nation, they shall be subject to the approval of a NATO Nation.

7.10.9. For the procurement of general purpose security-related and security enforcing products, the NATO Information Assurance Products Catalogue should be consulted.

---

[3] Not applicable to cryptographic and TEMPEST products.

[4] Procurement requirements for cryptographic products or mechanisms are specifically defined in relevant Technical and Implementation directives developed by C3B.

7.10.10. Managing trustworthiness in the supply chain, through which CIS handling classified information and related components are acquired, requires also that NATO classified information disseminated to industry, generated as a result of a contract with industry, and classified contracts with industry shall be protected in accordance to the requirements set in Enclosure "F" of the Policy on Security within the North Atlantic Treaty Organisation and supporting directives.

7.11. **Security design of CIS**

7.11.1. Security models and security architectures shall be used to specify how the Policy on Security within the North Atlantic Treaty Organisation and supporting directives are enforced in NATO CIS and how the security objectives are achieved.

7.11.2. For CIS handling NATO classified information the indication of the security mode of operation shall be used to describe the security conditions under which the system operates.

7.11.3. **Security Modes of Operation**

7.11.3.1. NATO CIS handling information classified NATO CONFIDENTIAL and above, or Special Category information shall operate in one, or where warranted by requirements during different time periods, more than one, of the following security modes of operation:

(a) "dedicated" – a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, and with a common need-to-know for all of the information handled within the CIS;

(b) "system high" - a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, but not all individuals with access to the CIS have a common need-to-know for the information handled within the CIS; approval to access information may be granted at an informal or individual level;

(c) "compartmented" - a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, but not all individuals with access to the CIS have a common need-to-know and formal authorisation[5] to access all of the information handled within the CIS;

(d) "multi-level" - a mode of operation in which not all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, and not all individuals with access to the CIS have a common need-to-know for all of the handled within the CIS.

[5] Formal authorisation indicates that there is a formal central management of access control as distinct from an individual's discretion to grant access.

7.11.3.2. NATO CIS handling NATO RESTRICTED or below information shall operate in one, or where warranted by requirements during different time periods, more than one, of the following security modes of operation[6]:

(a) "dedicated" - a mode of operation in which all individuals with access to the CIS have a common need-to-know for all of the information handled within the CIS;

(b) "system high" - a mode of operation in which all individuals with access to the CIS do not have a common need-to-know for all of the information handled within the CIS;

(c) "compartmented" - a mode of operation in which all individuals with access to the CIS do not have a common need-to-know and formal authorisation to access all of the information handled within the CIS.

7.11.3.3. The Information Category Designation, US-Single Integrated Operation Plan (SIOP), shall only be processed in the "dedicated" security mode of operation.

7.12. **Interconnection of CIS**

7.12.1. Very often, in order to fulfil their mission, organisations require interconnecting their CIS to CIS of different organisations, communities of interest, security classifications and security postures. In order to safeguard the security principle of self-protecting CIS, it is necessary addressing the potential risks posed by interconnecting, directly or through a cascading interconnection, a CIS handling NATO information to another CIS and implementing specific security measures to control the interconnection.

7.12.2. For all interconnections of NATO CIS and other CIS handling NATO classified information, the following shall be subject to the approval of the SAA or designated NATO authority for NATO CIS handling non-classified information:

(a) the method of interconnection and services provided;

(b) where appropriate, the security risk assessment and risk management methodology to be utilised, and the results of the security risk assessment;

(c) the security architecture and security measures for ensuring the achievement of the security objectives;

(d) the security-related documentation, including the security test plan and the results of the security testing.

7.12.3. The supporting CIS Security Management directive sets out the specific security accreditation requirements and the supporting technical and implementation directives on CIS Security define the specific measures to be implemented.

---

[6] These interpretations of the modes of operation are included to show that a security clearance is not required for access to NATO RESTRICTED information.

7.12.4. The requirement for protective measures for CIS handling NATO information which are interconnected to Internet or similar networks in the public domain arises from the exceptional security risks posed by these types of public networks through their pervasive uncontrollable world-wide accessibility and the inherent susceptibility of their connectionless-oriented protocols and the vulnerabilities of the end CIS to exploitation. Especially CIS handling NATO classified information are at unacceptable security risk unless specifically protected.

7.12.5. The direct or cascaded interconnection to Internet or similar networks in the public domain of NATO CIS and other CIS handling NATO classified information up to and including NATO SECRET shall be:

(a) strictly controlled;

(b) be subject to the requirements of the SAA or designated NATO authority for NATO CIS handling non-classified information;

(c) be subject to evaluation and certification and/or approval of the security enforcing mechanisms as identified by relevant technical and implementation directives on CIS Security issued by C3B and by the SAA or designated NATO authority for NATO CIS handling non-classified information;

(d) be subject to periodic and formal vulnerability assessments.

7.12.6. The direct or cascaded interconnection of CIS handling information classified COSMIC TOP SECRET, and/or Special Category information, to Internet or similar networks in the public domain is prohibited.

7.12.7. **NATO information on Internet or similar networks in the public domain**

7.12.7.1. CIS handling NATO classified information may use the Internet or similar networks in the public domain purely as a bearer, provided that the appropriate cryptographic protection is implemented. In this instance, all security objectives shall be seriously considered.

7.12.7.2. The only information which may be transmitted in clear (i.e., non-encrypted) text is the following:

(a) open source and public information, or NATO information specifically approved for disclosure to the public; and

(b) non-sensitive NATO UNCLASSIFIED; i.e., information that, as determined by the originator(s), bears no additional administrative marking (for example, medical,) or dissemination limitation marking to indicate the sensitivity of the information.

7.12.7.3. Only open source and public information, or NATO information specifically approved for disclosure to the public, may be posted on publicly-accessible bulletin boards or web pages and shall be subject to the integrity requirements of the originator(s) of the information.

7.13. Application security

7.13.1. Security shall be embedded in the life-cycle (design, development, deployment, maintenance) of bespoke software purposely developed to handle NATO information, by taking into account the security objectives defined for the CIS.

7.13.2. Applications shall be subject to security testing, configuration management (e.g. baselines) and change control (e.g. patching), processes which shall be designed and managed by the CISP, in close coordination with the SAA or designated NATO authority for NATO CIS handling non-classified information, to ensure that the CIS Security objectives are properly taken into account.

7.13.3. On NATO CIS, CISPs shall maximise the use of automated tools to support application white listing and vulnerability detection.

7.14. Cryptographic security

7.14.1. The requirements relevant to cryptographic security are set in Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation and in the related technical and implementation directives issued by C3B.

7.15. Emission security

7.15.1. The requirements relevant to emission security are set in Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation and in the related technical and implementation directives issued by C3B.

7.16. Third party service delivery

7.16.1. For NATO CIS and other CIS handling NATO classified information, especially when outsourced, the CISP and the CISOA, in coordination with the SAA or designated NATO authority for NATO CIS handling non-classified information, shall formally agree (e.g. service level agreements, contracts) the requirements for implementation, management, monitoring and change management of CIS Security measures.

7.17. Security related logs

7.17.1. NATO CIS and other CIS handling NATO classified information shall be protected by security measures for the detection of malicious activities and faults, through the collection, review and storage of information for security related events.

7.17.2. Measures are required in order to provide sufficient information, including traceability of events, to be able to investigate a deliberate, accidental or attempted compromise of the security objectives of a CIS, commensurate with the damage that would be caused.

7.17.3. The requirements for collection of information for security related events shall also be defined by taking into account that security logs are fundamental to support the activity of security audit by SAAs.

7.17.4. The review and retention period for security logs shall be defined by the SAA or designated NATO authority for NATO CIS handling non-classified information, in coordination with the CISP and CISOA, based on a risk management approach which considers, among any other factor considered relevant by the authority responsible of the security accreditation, the following:

(a) security objectives of the CIS;

(b) threat environment;

(c) type of logs and data collected;

(d) frequency of log reviews;

(e) use of automated tools in support of log verification;

(f) investigative, audit and legal requirements.

7.18. **Security baselines**

7.18.1. On NATO CIS and other CIS handling NATO classified information, security baselines for CIS and critical hardware and software shall be defined, enforced and kept up-to-date through configuration management and change control during the entire CIS life-cycle.

7.18.2. Security baselines shall include security settings required to harden the configuration of critical components before deployment and requirements for security updates for components in operation.

7.18.3. On NATO CIS, CISPs shall maximize the use of automated tools for vulnerabilities discovery and remediation as well as produce implementation plans relevant to security baselines for the SAA’s approval.

7.19. **Malware defence**

7.19.1. Although malicious software has always been recognised as a challenging threat, its evolution in sophistication and its ability to execute targeted attacks require high attention.

7.19.2. On NATO CIS and other CIS handling NATO classified information, dependent upon the security objectives of the CIS, malicious code detection solutions shall be utilised to block installation, prevent execution, quarantine malicious software and alert personnel responsible for incident response related activities.

7.20. **Access control**

7.20.1. Access control is a first line of defence as it allows the identification, authentication, authorisation and accountability of any entity (e.g. person, device, service) requesting access to a CIS and its elements.

7.20.2. On NATO CIS and other CIS handling NATO classified information, access control measures shall be implemented to prevent unauthorised operations on the CIS and related elements (e.g. data, devices, services).

7.20.3. In the selection of an access control model and its related security measures, CISPIA shall consider the following factors:

(a) the way and the extent to which an organisation implements information management may have an impact on the design of access control measures;

(b) technical measures shall be designed in the context of the overall security environment of a CIS to work in a coherent and coordinated manner with physical and administrative access control measures;

(c) technical measures shall enable secure and granular access to information based on the security mode of operation for which the CIS has been intended and on the validated requirements for the sharing of information among the communities of interests within the CIS and with other CIS.

7.20.4. Traditional network boundaries are a major element for the security design of a CIS infrastructure. However CISPIA shall also take into account that these boundaries cannot be considered an exhaustive point of reference when protecting NATO classified information handled in CIS with complex information sharing and access control requirements. This is typical of CIS such as those hosting communities of interest of different trust categories, federating with other CIS or implementing new concepts as in the case of cloud-computing.

7.20.5. Particularly in such scenarios, CISPIA shall adopt defence in-depth strategies which include security policies and measures specific for the protection of information objects based on the identity and other relevant attributes of the entity requesting access to the object as well as the properties of that object, commonly termed metadata labels.

7.20.6. Where access by non-NATO nationals to NATO CIS is authorised, measures shall be applied to restrict access only to the NATO classified information essential to NATO’s mission. The appropriate NATO SAA shall exercise oversight of those measures,

including the review of the periodic reassessment of the security risks associated with access by non-NATO nationals to NATO CIS.

7.20.7. In the context of access control, Identity and Access Management (IAM) plays a fundamental role as it comprises of the people, processes and products necessary to manage digital identities (e.g. person, device, service and data), throughout their life-cycle, and the access to CIS resources.

7.20.8. For NATO CIS, access to CIS resources shall be managed through enterprise IAM capabilities that

(a) manage digital identities and their attributes, privileges and credentials;

(b) provide authentication services, including strong authentication, when indicated by risk management;

(c) prevent credential theft and reuse;

(d) provide granular authorization based on access policies;

(e) audit users and systems activities.

7.20.9. Minimum requirements for identification and authentication on NATO CIS and other CIS handling NATO classified information are set in the technical and implementation directives on CIS Security issued by C3B and shall, where appropriate, be determined as a result of a risk management process. Requirements for identification and authentication shall define the characteristics of the mechanisms and the extent to which these mechanisms shall be implemented and assured.

7.21. **Incident response**

7.21.1. A CIS Security incident is any detected anomaly compromising or that has the potential to compromise communication, information or other electronic systems or the information that is stored, processed or transmitted in these systems.

7.21.2. Technically oriented security management staff shall be designated and available to address security incidents.

7.21.3. Incidents related to CIS Security shall be reported for response, investigative and inspection purposes in accordance with the requirements of relevant CIS Security directives and of the SAA or designated NATO authority for NATO CIS handling non-classified information.

7.21.4. CIS Security related incidents affecting NATO CIS shall be notified to the NATO Computer Incident Response Capability (NCIRC) and/or the responsible CIS Security Officer, in compliance with the Internal Security Instructions (ISIs) or Security Operating Procedures (SecOPs) of NATO civil or military bodies and in accordance with the incident reporting formats and guidelines defined by the NCIRC and/or security investigative authorities.

7.21.5. The Directive on the Security of Information describes the conditions under which NOS shall be immediately notified that an incident has occurred for security investigative purposes and shall receive relevant reports. For NATO CIS, the Primary Directive on CIS Security extends these conditions to the following cases:

(a) Security breach involving COSMIC TOP SECRET, NATO SECRET and Special Category information

(b) Unauthorised disclosure of NATO classified information to media (e.g. press, blogs, websites) or other entities (e.g. political, terrorist and criminal groups);

(c) Unauthorised major data harvesting;

(d) Suspected espionage;

(e) Internal malicious activity (e.g. insider threat);

(f) Incidents involving privileged access to CIS;

(g) Incidents involving cryptographic elements;

(h) Incidents causing a significant impact to the organisation.

7.21.6. All other CIS Security incidents affecting NATO CIS and investigated by the relevant NATO security authorities shall be notified to NOS for oversight, analytical and statistical purposes.

7.21.7. Identification, collection, acquisition and preservation of potential digital evidence shall be undertaken by personnel trained in forensics procedures, in a systematic and impartial manner for preserving its integrity, authenticity and admissibility in accordance with relevant legal and policy requirements.

7.22. **Security Management Infrastructure**

7.22.1. Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation requires that security management mechanisms and procedures shall be in place to deter, prevent, detect, withstand and recover from, the impact of incidents affecting NATO classified information and CIS. To this end, a Security Management Infrastructure (SMI) shall be established to ensure that the capabilities managing CIS Security related services, processes and devices across NATO bodies are managed as an enterprise.

7.23. **CIS Security Training and Awareness**

7.23.1. A major factor in achieving an adequate security posture of a CIS is an active security education and awareness programme for all CIS users.

7.23.2. Security education and awareness programme shall make users aware of the general threats and vulnerabilities applicable to the CIS they use, in order that they understand the rationale for, and acknowledge their responsibility to maintain,

the protective security measures in place. Special care shall be given to emergent and particular threats (e.g. targeted attacks, social engineering and insider threat) as these exploit the weaknesses of the human behaviours.

7.23.3. CIS Security education and awareness shall be provided to senior level management, CIS planning, implementing and operating staffs, security staffs and users to ensure that security responsibilities are clearly understood. To this end, minimum CIS security training standards for personnel shall be identified.

Appendix 1 - Roles and Responsibilities of NATO and national bodies involved in CIS Security

1. National authorities and agencies

(a) National Security Authorities (NSA);

(b) Designated Security Authorities (DSA);

(c) National Communication Security Authorities (NCSA);

(d) National Tempest Authorities (NTA);

(e) National Distribution Authorities (NDA);

(f) National Security Accreditation Authorities (SAA).

2. NATO bodies

2.1. Under the ultimate authority of the North Atlantic Council (NAC), NATO Committees and their sub-structures, Commands, Agencies and Staffs may be identified as follows:

(a) NATO bodies directly responsible for CIS Security policy, directives and guidance:

i. the Security Committee (SC) and the Security Committee in CIS Security Format (SC(CISS)) where National Security Authorities (NSAs) and Designated Security Authorities (DSAs) are represented;

ii. the C3 Board (C3B), and its Capability Panel on Information Assurance and Cyber Defence (CaP4);

iii. the Military Committee (NAMILCOM) for military requirements;

iv. various NATO civil committees for their civil requirements.

(b) NATO bodies indirectly concerned with CIS Security resources:

i. the financial committees, Senior Resource Board (SRB), the Resource Policy and Planning Board (RPPB), the Budget Committee (BC) and the Investment Committee (IC);

ii. the NATO Defence Manpower Committee for personnel aspects, in military establishments.

(c) NATO staff support in NATO Headquarters:

i. the NATO Office of Security (NOS);

ii. the NATO Headquarters C3 Staff (NHQC3S) and its Information Assurance and Cyber Defence Branch;

iii. the International Staff (IS), including the Emerging Security Challenges Division (ESC) and its Cyber Defence Section, and International Military Staff (IMS).

(d) NATO bodies representing the users:

i. Supreme Headquarters Allied Powers Europe (SHAPE) and HQ Supreme Allied Commander Transformation (SACT) for users in military establishments;

ii. specific civil agencies for civil users.

(e) NATO bodies responsible for operational and technical support to CIS Security policy, direction and implementation bodies:

i. Supreme Headquarters Allied Powers Europe (SHAPE) and HQ Supreme Allied Commander Transformation (SACT) for military establishments;

ii. the four nationally manned Military Committee agencies, for security evaluation of cryptographic products, vulnerability assessment of CIS, keying material distribution and accounting:

- Communications and Information Systems Security and Evaluation Agency (SECAN) - organised and staffed by the United States;
- Distribution and Accounting Agency (DACAN) - organised and staffed by the United States;
- European Communications Security and Evaluation Agency (EUSEC) - organised and staffed by the United Kingdom;
- European Distribution and Accounting Agency (EUDAC) - organised and staffed by the United Kingdom.

iii. the NATO Communications and Information Agency (NCI Agency) for the provision of communications and information systems and services;

iv. the NATO School (NSO) and the NATO CIS School (NCISS) for education and training;

v. the NATO Public Key Infrastructure (PKI) Management Authority (NPMA);

vi. the NATO CIS Security Accreditation Board (NSAB);

vii. the NATO Cyber Defence Management Board (CDMB).

2.2. **Security responsibilities**

2.2.1. The security responsibilities of the Security Committee (SC), the NATO Office of Security (NOS), the NATO Military Committee (NAMILCOM) and NATO Military bodies, the C3 Board (C3B), NATO Civil bodies, National Security Authorities (NSAs) and

Designated Security Authorities (DSAs) are addressed in the Policy on Security within the North Atlantic Treaty Organisation. The responsibilities of NATO committees, NATO Civil and Military bodies, and National bodies with NATO CIS Security responsibilities are addressed in the appropriate NATO and National documents, including official Terms of Reference (TORs).

Appendix 2 - CIS Security-related Activities in the CIS Life Cycle

1. Introduction

1.1. This section addresses the essential activities related to CIS Security, and their associated responsible authorities and staffs, which shall be undertaken during the life-cycle of NATO CIS and other CIS handling NATO classified information. These activities are based upon the requirements established in more detail in the supporting directives. The following generic stages of the CIS life-cycle are identified, which may be adapted according to NATO and national requirements:

(a) CIS planning;

(b) CIS development and procurement;

(c) CIS implementation and security accreditation;

(d) CIS operation

(e) CIS enhancement;

(f) CIS withdrawal from service, and disposal of equipment.

1.2. The activities related to CIS Security highlight the context in which the Policy on Security within the North Atlantic Treaty Organisation and its supporting directives and guidance on management as well as technical and implementation aspects are to be utilised, in order to assess the security accreditation, and implementation requirements.

2. **CIS Planning**

2.1. The following activities related to CIS Security and responsible authorities are associated with the planning stage of a CIS:

Activity	Responsible Authority / Staffs
1. Identify and notify the appropriate SAA, or designated NATO authority for NATO CIS handling non-classified information[7], of CIS plans	CISPIA
2. Establish or identify a CIS security framework necessary to meet security objectives of the CIS in questions and identify the tasks related to CIS Security	CISPIA, coordinating with CISP and SAA
3. Establish the basis for security accreditation through the development of a security accreditation plan or security accreditation strategy	CISPIA in close coordination with SAA
4. Approve the security accreditation plan or security accreditation strategy	SAA
5. For NATO CIS, identify the security risk assessment requirement and the security risk assessment and management methodology to be utilised	SAA, coordinating with CISPIA
6. For NATO CIS, undertake an initial security risk assessment in accordance with the requirements of the SAA	CISPIA in conjunction with CIS operational authority (CISOA), coordinating with the SAA

[7] For readability reason, from now on the term SAA is utilised to refer as well to the designated NATO authority for NATO CIS handling non-classified information, unless differently indicated.

Activity	Responsible Authority / Staffs
7. For NATO CIS, develop an initial security architecture based on the mission objectives and the findings of the initial security risk assessment	CISPIA in conjunction with CISOA, coordinating with SAA
8. For NATO CIS, approve the results of the initial security risk assessment	SAA, in coordination with CISOA
9. Identify initial requirement for products requiring evaluation and certification and/or approval (e.g. cryptographic products) and identify supply chain security requirements	CISPIA and, where appropriate, coordinating with SAA For NATO CIS this may require coordination also with C3B and its substructure
10. Identify initial requirement for security baselines, configuration management and change control	CISPIA, coordinating with the CISP and appropriate SAA
11. Identify initial requirement for training and awareness	CISPIA, coordinating with the appropriate SAA
12. Identify initial requirement for business continuity	CISPIA, in conjunction with the CISOA and in coordination with the SAA
13. Identify initial requirement for security logs retention	CISPIA, in conjunction with CISOA, CISP and SAA
14. Develop the initial Security Requirement Statements (SRS(s)) (or national equivalent(s)), or, where appropriate for NATO CIS, address the required CIS Security aspects of Capability Packages (CPs) and associated documents; using, where appropriate, applicable Protection Profiles (e.g. collaborative PP)	CISPIA, coordinating with SAA

Activity	Responsible Authority / Staffs
15. Approve the initial SRS(s) (or national equivalent(s)) or, where appropriate for NATO CIS, approve the required CIS Security aspects of Capability Packages (CPs) and associated documents	SAA

3. **CIS Development and Procurement**

3.1. The following activities related to CIS Security and responsible authorities are associated with the development and procurement stage of a CIS:

Activity	Responsible Authority / Staffs
1. For NATO CIS, refine the security risk assessment	CISPIA, in conjunction with SAA
2. Develop the security architecture and check it against reference security architecture(s) to ensure, where possible, security interoperability and integration of new CIS in existing infrastructure(s)	CISPIA
3. For NATO CIS, approve the results of the refined security risk assessment	SAA, in coordination with CISOA
4. Approve the security architecture	SAA
5. Develop a detailed specification of security measures covering personnel, physical, and security of information aspects	CISPIA, coordinating with CISP, site Security Authority, and SAA
6. Develop a detailed specification of CIS Security measures, in accordance with the requirements of the SAA, addressing security functionality and assurance and, where appropriate, the interconnection of CIS.	CISPIA, coordinating with CISP and SAA
7. Refine requirement for products requiring evaluation and certification and/or approval and security requirements for supply chain	CISPIA and, where appropriate, coordinating with appropriate SAA For NATO CIS this may require coordination also with C3B and its substructure

Activity	Responsible Authority / Staffs
8. Refine requirement for security baselines, configuration management and change control	CISPIA, in conjunction with the CISP and in coordination with appropriate SAA
9. Refine requirement for training and awareness	CISPIA, in coordination with the appropriate SAA
10. Refine requirement for business continuity	CISPIA, in conjunction with the CISOA and coordinating with appropriate SAA
11. Refine requirement for security logs retention	CISPIA, in conjunction with CISOA, CISP and SAA
12. Approve requirement for security baselines, configuration management and change control	SAA
13. Approve requirement for training and awareness	CISOA, in coordination with appropriate SAA
14. Approve requirement for business continuity	CISOA, in coordination with appropriate SAA
15. Approve requirement for security logs retention	SAA, in coordination with the CISOA
16. Approve security requirements for assured products and supply chain	SAA and, where appropriate, C3B

Activity	Responsible Authority / Staffs
17. Review CIS Security products lists for assured products which can meet the CIS security requirement(s) (e.g. NATO Information Assurance Product Catalogue)	CISPIA, coordinating with CISP and SAA
18. Where appropriate, develop the operational requirements for cryptographic products and mechanisms using, where appropriate, applicable protection profiles. For NATO CIS under NATO common funding, notify C3B and its substructure of requirements	CISPIA, coordinating with the CISP and SAA
19. Where appropriate, for NATO CIS under NATO common funding, develop the technical characteristics for cryptographic products and mechanisms	C3B and its substructure
20. Where appropriate, advise NCSAs, through C3B, of the requirement for cryptographic products and mechanisms	CISPIA
21. Where appropriate, establish an evaluation / selection timetable for cryptographic products and mechanisms	Supporting staffs of C3B and its substructure, coordinating with the NCSAs, SECAN, CISPIA, and CISP
22. Where appropriate, undertake evaluation, approval and selection of cryptographic products and mechanisms.	Supporting staffs of C3B and its substructure (supported by NCI Agency), in conjunction with SECAN, with approval by NAMILCOM
23. Establish requirement for Security Test and Verification (ST&V) of the CIS or, where appropriate, of the interconnection of CIS	SAA, coordinating with CISPIA.

Activity	Responsible Authority / Staffs
24. For NATO CIS, ensure that the Type "B" Cost Estimate (TBCE) identifies any requirement for all CIS Security related activities, including security accreditation and assurance activities (e.g. evaluation, certification, approval) in order to establish the appropriate funding	CISPIA, coordinating with SAA
25. On-going development of the SRS(s) (or national equivalent(s)); using, where appropriate, applicable Protection Profiles	CISPIA, coordinating with SAA
26. On-going approval of the SRS(s) (or national equivalent(s))	SAA
27. Ensure that the Service Level Agreement (SLA), established between the CISP and the CISOA for the provision of CIS services, addresses, as a minimum, the requirements for implementation and management of security measures as well as for monitoring and change management.	CISPIA, coordinating with SAA

4. CIS Implementation and Security Accreditation

4.1. The following activities related to CIS Security and responsible authorities are associated with the implementation and security accreditation stage of a CIS:

Activity	Responsible Authority / Staffs
1. Refine Security Test and Verification (ST&V) requirements of the CIS or, where appropriate, the interconnection of CIS	SAA, coordinating with CISPIA and CISP
2. Develop Security Test and Verification (ST&V) plan	CISPIA, coordinating with CISP and SAA
3. Undertake, where required, all activities necessary to obtain assured products, in accordance with, where appropriate, the evaluation methodologies approved by C3B or nationally or internationally equivalent methodologies	NATO or National[8] Authority responsible for evaluation, certification and/or approval of products, coordinating with the CISPIACISP
4. Undertake security testing, in accordance with an agreed ST&V plan	CISP, coordinating with the CISPIA and SAA
5. Review results of security testing	SAA
6. Identify any additional security countermeasures to be implemented if the result of the security testing is not satisfactory	CISPIA, coordinating with CISP and SAA
7. For NATO CIS, identify and agree the residual risks to be accepted	CISOA

[8] As determined by the National Security Authority.

Activity	Responsible Authority / Staffs
8. For NATO CIS, identify and agree the on-going security risk management processes	SAA, in conjunction with CISOA
9. Complete the SRS(s) (or national equivalent(s))	CISPIA, coordinating with SAA
10. Approve the SLA, established between the CISP and the CISOA for the provision of CIS services	CISOA and CISP
11. Formulate the Security Operating Procedures (SecOPs) (or national equivalent(s)) for the CIS	CISP, coordinating with security management staffs[9]
12. Approve the SRS(s) and SecOPs (or national equivalent(s))	SAA
13. Provide initial training and awareness	CISPIA or CISOA or CISP as appropriate
14. Accredit the CIS or, where appropriate, the interconnection of CIS and issue an accreditation statement which includes the period of validity of the accreditation	SAA
15. Establish the re-accreditation conditions	SAA

[9] Security Officer, CIS Security Officer, System and Network Administrator.

5. **CIS Operation**

5.1. The following activities related to CIS Security and responsible authorities are associated with the operation stage of a CIS:

Activity	Responsible Authority / Staffs
1. Authorise CIS to operate	CISOA
2. Store, process or transmit NATO information in the operational environment in accordance with the approved SecOPs (or national equivalent(s)), including system and security administration and in accordance to the specific service requirements included in relevant SLAs	CISP, coordinating with security management staffs
3. Maintain security baselines through configuration management and change control	CISP, in coordination with SAA
4. For NATO CIS, perform on-going security risk management, in accordance with the requirements of the SAA. This includes reporting to senior management and the SAA on changes in the risk posture due to evolving threats and vulnerabilities as well as to changes of the CIS status (e.g. value, configuration, compliance to security baselines, physical and personnel security measures).	CISOA, coordinating with CISP and SAA

Activity	Responsible Authority / Staffs
5. Detect, react to and report on CIS Security incidents, in accordance with the requirements of relevant NATO security policies and directives, the SecOPs (or national equivalent(s)) and with relevant procedures established by the Cyber Defence Management Board and/or security investigative authorities.	CISOA and CISP, coordinating with SAA
6. Provide regular training and awareness	CISOA or CISP as appropriate
7. Undertake, in accordance with the requirements of the SAA, periodic vulnerability assessments and, on NATO CIS, maximise the use of automated tools to continuously assess CIS compliance to security baselines.	CISP or a separately established vulnerability assessment team, coordinating with SAA and CISOA
8. Undertake, in accordance with NATO security policy, periodic security audits of the CIS or, where appropriate, the interconnection of CIS	SAA, coordinating with CISOA and CISP

6. **CIS Enhancement**

6.1. The following activities related to CIS Security and responsible authorities are associated with the enhancement stage of a CIS:

Activity	Responsible Authority / Staffs
1. Undertake, where required by an update of an assured product, all activities necessary to obtain re-assurance (e.g. evaluation, certification and approval) for the new product, in accordance with, where appropriate, the evaluation methodologies approved by C3B or nationally or internationally equivalent methodologies	NATO or National[10] Authority responsible for evaluation, certification and/or approval of products, coordinating with CISPIA, CISP and SAA
2. For NATO CIS, refine the security risk assessment	CISPIA, in conjunction with the CISOA, CISP and SAA
3. Revise the security architecture and check it against reference security architecture(s) to ensure, where possible, security interoperability and integration of new CIS in existing infrastructure(s)	CISPIA
4. For NATO CIS, approve the results of the refined security risk assessment	SAA, in coordination with CISOA
5. Re-approve the security architecture	SAA
6. Identify any required changes to security countermeasures.	CISPIA, in conjunction with CISP and SAA
7. Identify required changes to training and awareness	CISPIA or CISOA or CISP as appropriate

[10] As determined by the National Security Authority.

Activity	Responsible Authority / Staffs
8. Identify required changes to business continuity requirements	CISOA in coordination with appropriate SAA
9. Identify required changes to security logs retention requirements	CISPIA, in conjunction with CISOA, CISP and SAA
10. Establish requirement for ST&V of the CIS or, where appropriate, of the interconnection of CIS	SAA, coordinating with CISPIA and CISP
11. Develop ST&V plan	CISPIA, coordinating with CISP and SAA
12. Undertake security testing, in accordance with an agreed ST&V plan	CISP, coordinating with CISPIA and SAA
13. Review results of security testing	SAA
14. Identify, as a result of the security testing, any additional security countermeasures to be implemented	CISPIA, coordinating with SAA and CISP
15. For NATO CIS, review and agree the residual risks to be accepted	CISOA
16. For NATO CIS, review and agree the on-going security risk management processes	SAA, in conjunction with CISOA
17. Revise the SRS(s) (or national equivalent(s)); using, where appropriate, applicable Protection Profiles	CISP, coordinating with SAA

Activity	Responsible Authority / Staffs
18. Revise the SecOPs (or national equivalent(s)) for the CIS	CISP, coordinating with the security management staffs and SAA
19. Re-approve the SRS(s) and SecOPs (or national equivalent(s))	SAA
20. Re-accredit the CIS or, where appropriate, the interconnection of CIS; and re-publish an accreditation statement	SAA
21. Review and re-establish the re-accreditation conditions	SAA

7. CIS Withdrawal from Service and Disposal of Equipment

7.1. The following activities related to CIS Security and responsible authorities are associated with the withdrawal from service, and disposal of equipment stage of a CIS:

Activity	Responsible Authority / Staffs
1. Identify items that require archiving and/or de-classification and/or disposal and/or destruction and related requirements	CISOA and/or CISP
2. Initiate the appropriate archiving or de-classification and destruction of associated fixed and removable computer storage media, and information required for accounting purposes	CISOA and/or CISP
3. Initiate the appropriate procedures for the disposal and/or destruction of special purpose equipment including cryptographic products and systems and their associated material	CISOA and/or CISP
4. Initiate the appropriate archiving or destruction of associated hard copy documentation	CISOA and/or CISP

Appendix 3 - NATO CIS Security Documentation Structure

1. This “Primary Directive on CIS Security” is supported by a number of CIS Security directives and guidance documents addressing CIS Security management, and CIS Security technical and implementation aspects. A "Roadmap" to the Policy on Security within the North Atlantic Treaty Organisation, supporting directives, supporting documents and guidance documents is published by the NATO Office of Security and the NATO HQ C3 Staff respectively on behalf of SC and the C3B. The Roadmap may also be accessed on the NATO SECRET Wide Area Network (WAN) at the NOS portion of the NATO HQ web site.

2. The "Roadmap" provides access to the following :

(a) NATO UNCLASSIFIED and NATO RESTRICTED documents published by the NAC, DPPC, the SC and the C3B, with respect to information management, security and cyber defence;

(b) contact information of NATO and National Security Authorities.