

NATO UNCLASSIFIED

12 October 2015

DOCUMENT
AC/35-D/2005-REV3

SECURITY COMMITTEE

MANAGEMENT DIRECTIVE ON CIS SECURITY


Note by the Chairman

1. At Annex 1 is the "Management Directive on CIS Security" that is published by the Security Committee in support of NATO Security Policy (C-M(2002)49) and the Primary Directive on CIS Security (AC/35-D/2004-REV3).
2. This directive has been approved by the Security Committee in CIS Security format under silence procedure (AC/35-WP(2015)0004)-AS1 (CISS) refers) and will be subject to periodic review.
3. This document replaces AC/35-D/2005-REV2 which should be destroyed.

(Signed) Marco Criscuolo

Annex: 1

Action officer: Josef Holubík, NOS/POB, ext. 5043

Original:  519017300

NATO UNCLASSIFIED

MANAGEMENT DIRECTIVE ON CIS SECURITY

Contents

1. **Introduction** 1-3

2. **Purpose**..... 1-3

3. **Scope** 1-3

4. **CIS Security Roles and Responsibilities** 1-4

 4.1. **General**..... 1-4

 4.2. **Security Accreditation Authority**..... 1-4

 4.3. **CIS Planning and Implementation Authority** 1-6

 4.4. **CIS Provider**..... 1-7

 4.5. **CIS Operational Authority**..... 1-7

 4.6. **Security Management Staff** 1-8

5. **Security Accreditation of CIS** 1-11

 5.1. **General**..... 1-11

 5.2. **The Bases for Security accreditation**..... 1-12

 5.3. **Establishing a Security Accreditation Process**..... 1-13

 5.4. **Approval for testing** 1-13

 5.5. **Security Accreditation Outcome** 1-14

 5.6. **Ongoing Security Accreditation Activities** 1-14

6. **Security Risk Management for NATO CIS** 1-15

 6.1. **General**..... 1-15

 6.2. **The Security Risk Assessment and Risk Management Processes**..... 1-16

 6.3. **On-going Security Risk Management** 1-18

7. **Security-Related Documentation** 1-18

 7.1. **General**..... 1-18

 7.2. **Operational requirements for NATO CIS** 1-18

 7.3. **Security Risk Management Report for NATO CIS** 1-18

 7.4. **Security Architecture for NATO CIS**..... 1-19

 7.5. **Security Accreditation Plan/Security Accreditation Strategy** 1-19

 7.6. **Security Requirement Statements** 1-19

7.7. Role of an SRS 1-20

7.8. Types of SRS 1-21

7.9. Security Test and Verification Plan and Report 1-22

7.10. Security Operating Procedures 1-23

8 Security Accreditation of the Interconnection of NATO CIS 1-23

9 Assured CIS and security enforcing products 1-24

9.1 General 1-24

9.2 Evaluation and security accreditation for CIS 1-24

9.3 Evaluation, certification and approval of security enforcing products 1-25

10 Management of Security Implementation of CIS 1-27

10.1 General 1-27

10.2 Security Implementation Management Requirements 1-27

11 Security Audit of CIS 1-28

11.1 General 1-28

11.2 Types of Security Audits 1-28

11.3 Security Audit Requirements 1-30

Appendix 1 - General CIS Security Aspects 1-31

1. Introduction

1.1. CIS Security is a complex domain which encompasses both the management and technical activities necessary to achieve an appropriate level of protection for CIS handling NATO information, cope with the evolving threat environment and enable organisations to fulfil their mission.

1.2. The CIS Security management activities, which are identified in the Primary Directive on CIS Security, are disciplined further in this Directive by setting up roles, responsibilities and processes to be undertaken during the life-cycle of NATO CIS and other CIS handling NATO classified information.

2. Purpose

2.1. This directive is published by the Security Committee in CIS Security Format (SC(CISS)) in support of the NATO Information Management Policy (NIMP), the Policy on Security within the North Atlantic Treaty Organisation, the Enhanced NATO Policy on Cyber Defence and the Primary Directive on CIS Security, and addresses the following aspects:

- (a) CIS Security Roles and Responsibilities;
- (b) Security Accreditation of CIS;
- (c) Security Risk Management for NATO CIS;
- (d) Security-related Documentation;
- (e) Security Accreditation of the Interconnection of NATO CIS;
- (f) Assured CIS and security enforcing products;
- (g) Management of Security Implementation of CIS;
- (h) Security Audit of CIS;
- (i) General CIS Security Aspects.

3. Scope

3.1. This directive is applicable to security accreditation authorities (e.g. National Security Authorities (NSAs), Designated Security Authorities (DSAs) and NATO Security Accreditation Authorities (SAAs)), CIS Planning and Implementation Authorities (CISPIAs), CIS Operational Authorities (CISOAs), CIS Providers (CISPs), security management staff¹, project staff, host nations, and procurement authorities responsible for establishing and implementing CIS Security requirements, and for ensuring that CIS Security measures are maintained.

¹ Including Security Officer, CIS Security Officer, CIS Administrators.

3.2. This directive is mandatory and binding upon all NATO CIS and other CIS storing, processing or transmitting² NATO classified information³. 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. Where required, specific guidance is published in support of this directive. This directive shall be read in conjunction with the Policy on Security within the North Atlantic Treaty Organisation, the Enhanced NATO Policy on Cyber Defence, the Primary Directive on CIS Security and the directives addressing technical and implementation aspects of CIS Security, published by the C3B.

4. CIS Security Roles and Responsibilities

4.1. General

4.1.1. This section addresses the CIS Security-related roles and responsibilities of authorities/personnel involved in CIS Security during the life cycle of CIS. These roles include the SAA, the CISOA, the CISPIA, the CISP and security management staff. It is not excluded that some of these roles are played by the same organisational entity, however it is essential maintaining separation of duties between the SAA and all other roles.

4.2. Security Accreditation Authority

4.2.1. The SAA⁴ is responsible for performing the following functions:

- (a) providing advice and guidance on CIS Security policy and directives (and supporting security measures) to civil and military bodies, CISPIA, CISP, CISOA, security management staff, project staff, host nations and procurement authorities;
- (b) establishing a security accreditation process, clearly stating the security accreditation conditions for CIS under their authority and for the connections of external CIS to these CIS. Where appropriate, these requirements should be captured in a Security Accreditation Strategy (SAS). The security accreditation processes may vary depending upon circumstances, but shall be subject always to NATO security policy and its supporting directives;

² Hereafter referred to within this Directive as handling.

³ In this Directive the description “NATO CIS and other CIS handling NATO classified information” includes all NATO CIS including those handling non-classified information.

⁴ For NATO CIS handling non-classified information the following functions are responsibility primarily of the Head of the Civil and Military Body as established by the Primary Directive on CIS Security. The Primary Directive on CIS Security sets also the specific circumstances under which the security accreditation of a NATO CIS handling non-classified information is performed by a NATO SAA.

- (c) reviewing and approving security-related documentation, for example, security accreditation plans, security risk management reports, Security Requirement Statements (SRSs), security architectures, security implementation verification documentation (e.g. Security Test and Verification (ST&V) plans, vulnerability assessment reports) and Security Operating Procedures (SecOPs) or national equivalent security related documentation;
- (d) reviewing additional documentation, for example, concepts of operation, product certification reports, trusted facility manuals and security features user guides;
- (e) providing a statement of security accreditation for CIS, stating the conditions under which security re-accreditation is required. Where a statement of interim security accreditation is provided, the statement shall identify the conditions to be applied to the interim security accreditation and the activities required to achieve security accreditation;
- (f) checking the implementation of the security arrangements for the CIS under its responsibility, through security audits and primarily by undertaking periodic security inspections or reviews in accordance with the security accreditation process;
- (g) where applicable, liaising with CISPIA, CISP and CISOA in respect to security risk assessments, on-going security risk management and the acceptance of residual risks;
- (h) providing direction to the CISPIA, CISP, CISOA and security management staff in investigating any breach, or suspected breach, of the security arrangements and in assessing the damage caused;
- (i) providing advice/recommendations on corrective measures to be implemented (or recommending sources for appropriate advice);
- (j) advising the CISPIA, CISP and CISOA on the security risk and countermeasures implications of any proposed changes to the CIS;
- (k) exercising oversight of the CISP and CISOA in respect to the execution (e.g. scope, rules of engagement) and the results of ST&V and security audit related activities;
- (l) liaising with other SAAs in respect to interconnected CIS, for such purposes as agreeing System Interconnection Security Requirement Statements (SISRS) or national equivalent;

- (m) providing advice on the interconnection of NATO CIS and other CIS handling NATO classified information to any CIS;
- (n) where a CIS is required to use assured products, liaising and co-ordinating with the CISPIA and the appropriate National, International or NATO Evaluation Authority.

4.2.2. When a CIS falls under the responsibility of more than one SAA, all relevant SAAs shall exercise the functions mentioned above in a coordinated manner (e.g. establishing a Security Accreditation Board), where appropriate, to avoid an inharmonious approach to security accreditation.

4.3. CIS Planning and Implementation Authority

4.3.1. The CISPIA is responsible for performing the following CIS Security-related functions:

- (a) develop the Security Accreditation Plan (SAP) and submit it to the relevant SAA for its approval; where the SAA has developed a relevant Security Accreditation Strategy (SAS) the SAP shall be developed in accordance to its requirements;
- (b) establishing the CIS Security technical and implementation aspects for CIS, in conjunction with the CISP, CISOA, security management staff, project staff and the SAA;
- (c) providing advice and guidance on CIS Security technical and implementation aspects of CIS to the SAA;
- (d) advising the CISP of CIS Security 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 handled;
- (e) defining the CIS Security design requirements (e.g. network and operating system security requirements, boundary protection component requirements, malicious software prevention requirements) in operational requirements for CIS;
- (f) defining the CIS Security resource requirements (e.g. manpower) in operational requirements for CIS.

4.4. CIS Provider

4.4.1. The CISP is responsible for performing the following CIS Security-related functions:

- (a) formulating, and keeping under review, the security-related documentation required by the SAA in respect to the CIS under its responsibility;
- (b) providing proposals on the CIS Security measures to be implemented, in close co-operation and consultation with the CISPIA and the SAA, and ensuring that the agreed CIS Security measures are implemented;
- (c) establishing, as early as possible in the CIS life-cycle, the resources required to fulfil day-to-day CIS Security management functions;
- (d) ensuring that arrangements are made for adequate and appropriate CIS Security training at the very early stage of the CIS life-cycle;
- (e) providing the required evidence to the SAA in order that security accreditation can be carried out in an effective manner, and requesting security re-accreditation in accordance with the requirements of the security accreditation process;
- (f) operating and supporting the implemented CIS Security measures in accordance with the conditions of the given security accreditation;
- (g) checking, periodically or in real-time, the implementation of CIS Security measures (e.g. ST&V, vulnerability assessment) to ensure that the security posture of the CIS is consistent with the requirements of the SAA;
- (h) reporting to the SAA on the status of the CIS in accordance with the requirements of the security accreditation process.

4.5. CIS Operational Authority

4.5.1. The CISOA is responsible for performing the following CIS Security-related functions:

- (a) defining the business and operational requirements, operating principles and concept of operation of a CIS, including the information exchange requirements;

- (b) liaising, where applicable, with the CISPIA and the SAA during the development of the security risk assessment process for a CIS to provide inputs to the assessment and to set specific requirements;
- (c) accepting formally the residual risk, where applicable, resulting from the security risk assessment process and agreeing on a plan to manage the residual risk. With the exclusion of the exceptional circumstances defined in paragraphs 11.6 and 11.7 of Enclosure F to the Policy on Security within the North Atlantic Treaty Organisation, the CISOA shall not accept a level of risk higher than that considered acceptable by the SAA through the approval of the security risk assessment;
- (d) ensuring that the Service Level Agreements (SLA) or similar mechanisms, established with the CISP for the provision of CIS services, includes the requirements for implementation, operation, monitoring and change management of security measures;
- (e) conducting operational evaluation of the CIS and validating/authorising the CIS for operational use, once the security accreditation is granted by the SAA;
- (f) investigating, in conjunction with the SAA and the CISP, breaches or suspected breaches of security within the CIS, assessing the damage caused and reporting the conclusions to the SAA. The Head(s) of the organisation(s) identified as the CISOA(s) for the NATO CIS or the entity who has overall responsibility for the investigation for National CIS handling NATO classified information, shall identify a leading investigating authority (e.g. Security Officer, CIS Security Officer, Counter-Intelligence Officer, NSA, SAA) and determine who should participate in the process based on the nature of the incident.

4.5.2. When a CIS is provided at the level of an enterprise where more than one CISOA is established, all CISOAs using the CIS for their mission shall exercise the functions mentioned above in a coordinated manner (e.g. establishing a CISOA Board), where appropriate, to avoid inharmonious approach in the enterprise environment.

4.6. Security Management Staff

4.6.1. Security management staff include all those roles that perform CIS Security-related functions and support the security organisation of NATO and National bodies protecting NATO classified information to maintain security within their establishment. Those roles include, among others, the CIS Security Officer and the CIS Administrators.

4.6.2. The security organisation (e.g. Security Officer) is responsible for performing the following functions:

- (a) ensuring the correct implementation and maintenance of the protective measures (e.g. physical security, personnel security, security of information, industrial security) of the overall security environment in which the CIS is located and which may have a bearing on the security posture of the CIS;
- (b) verifying the security accreditation statements for any CIS in use to ensure that this achieve and maintain an appropriate security accreditation status;
- (c) ensuring that regular security audits are conducted to verify that CIS Security measures are implemented and maintained in accordance with the NATO Policy on Security within the North Atlantic Treaty Organisation and its supporting directives.

4.6.3. The CIS Security Officer, working under the direction of the security organisation, is responsible for performing the following functions:

- (a) formulating and maintaining SecOPs (or national equivalent) for the CIS, and circulating the SecOPs to CIS administrators and users on a periodic basis;
- (b) providing CIS Security advice to, and maintaining CIS Security awareness of, CIS administrators and users, including managers;
- (c) 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 security clearance, where required, and need-to-know for the information handled in the CIS;
- (d) ensuring that CIS administrators and users change their own passwords periodically;
- (e) checking the implementation and maintenance of hardware, firmware and software modifications and enhancements to the CIS to ensure that security is maintained;
- (f) 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 relevant NATO regulations;

- (g) ensuring the proper custody of computer storage media as well as 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;
- (h) ensuring that computer storage media to be released only contain that information authorised for release;
- (i) 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 Policy on Security within the North Atlantic Treaty Organisation and its supporting directives;
- (j) checking security related logs for event/process failure, and unauthorised user and system activity;
- (k) conducting or coordinating the execution of periodic security assessment of CIS (e.g. risk assessment, ST&V, security inspection, vulnerability assessment);
- (l) ensuring the implementation and regular testing of business continuity measures for the CIS (e.g. back-up and recovery) in accordance to the objectives of the organisation's overall Business Continuity Plan;
- (m) reporting to the CISOA, CISP and the SAA on any detected CIS security weaknesses and vulnerabilities;
- (n) managing and investigating CIS Security incidents in close coordination with the security organisation (e.g. Security Officer), the CISOA, the CISP, the SAA and, where required, the incident responder (e.g. National Computer Emergency Response Team, NATO Incident Response Capability) and the appropriate counter-intelligence authority, and reporting the conclusions to the SAA, through the established management structure.

4.6.4. Assigning the functions described above at paragraphs 4.6.2 and 4.6.3 to the same individual (e.g. Security Officer) could be considered by senior management, in coordination with the SAA, based on judgement of the workload and the available expertise.

4.6.5. The delineation of CIS Security functions between the security management staff of the CISOA and CISP shall be determined and formally agreed (e.g. through SLA) based on the responsibilities of the CISOA and CISP in respect to the CIS.

4.6.6. Segregation of duties shall be maintained between the CIS administrators and the security organisation, including the Security Officer and the CIS Security Officer. Further segregation of duties among CIS administrators (e.g. system, network, application, security) shall be considered during the security accreditation process.

4.6.7. CIS administrators are responsible for managing the CIS in accordance with relevant NATO policies and directives, the approved security-related documentation (e.g. SecOPs) and the specific service requirements included in the relevant SLAs.

5. Security Accreditation of CIS

5.1. General

5.1.1. This section deals with the requirements for the security accreditation of CIS. NATO security policy requires that NATO CIS and other CIS handling NATO classified information shall be subject to a security accreditation process.

5.1.2. The primary objective of security accreditation is to ensure that an adequate level of protection is achieved and maintained throughout the life cycle of the CIS. This includes ensuring that the CIS conforms to NATO security policy and supporting directives, and the CIS-specific security-related documentation.

5.1.3. The security accreditation requirements shall be established by the SAA, based on the high level provisions of this Directive and reflecting inter alia the mission criticality, the security objectives, the architecture of the CIS (e.g. stand-alone PC versus WAN) and the operational environment in which the CIS operates.

5.1.4. The security accreditation of NATO CIS and other CIS handling NATO classified information shall follow a structured process based on the high level requirements established in this Directive. Deviations from this structured process shall always be documented and can only be authorised by the appropriate SAA.

5.1.5. When exercised by an SAA, delegation of the security accreditation authority shall be formally documented and be in accordance with the following conditions:

- (a) the scope and conditions of the delegation shall be clearly defined;
- (b) the delegated authority accepts the additional tasks and duties related to the security accreditation and for this remains accountable to the delegating SAA;
- (c) the delegated authority uses qualified and experienced CIS Security personnel appropriately independent from the CISP;

- (d) the delegating SAA maintains its responsibilities and exercises them, as an example, primarily through supervision and periodic verification of the security accreditation processes carried out by the delegated authority.

5.1.6. The security accreditation of those NATO CIS handling non-classified information for which the Primary Directive on CIS Security assign responsibility to Heads of NATO Civil and Military Bodies can only be delegated to NATO SAAs;

5.1.7. When permitted by national laws and regulations, the delegation of security accreditation for NATO Nations' industrial CIS handling NATO RESTRICTED information shall be exercised exclusively in accordance with the specific requirements of the Directive on Classified Project and Industrial Security.

5.2. The Bases for Security accreditation

5.2.1. The primary bases for security 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 architecture, where applicable, to verify compliance to the Policy on Security within the North Atlantic Treaty Organisation and supporting directives, validate the achievement of the security objectives and ensure, where possible, security interoperability and integration of new CIS in existing infrastructure;
- (c) an assessment of the security-related documentation (e.g. SAP, Security Risk Management Report, SRS, ST&V plan, and SecOPs) (or national equivalent security-related documentation);
- (d) a verification that the security measures⁵, including security baselines, have been implemented, and are being maintained, in accordance with the security requirements (e.g. review of the results of security testing, and security inspection);
- (e) an assessment of the security posture of the CIS through security audit related activities;
- (f) for NATO CIS, an identification of the residual risk and the ongoing security risk management processes.

5.2.2. The SAA shall, in conjunction with the CISPIA and CISP, establish the requirements for security implementation verification (e.g. security testing, security

⁵ Personnel security, physical security, security of information and CIS Security controls.

inspection, vulnerability assessment) for specific CIS implementations and interconnections, based upon the established security accreditation process.

5.2.3. Security implementation verification includes confirming, through appropriate security testing (based upon an agreed ST&V plan), that the CIS Security measures are implemented and perform as required. In certain instances, the NATO security policy and the SAA require the CIS Security features to be subject to evaluation and/or certification and/or approval, based on NATO criteria (or nationally/internationally approved equivalent).

5.3. Establishing a Security Accreditation Process

5.3.1. The SAA shall establish a security accreditation process for those CIS within its domain. The CISPIA and CISP of the CIS to be accredited shall provide evidence of security compliance to be used during the security accreditation process. The security accreditation process may vary depending upon circumstances, but shall always be subject to NATO security policy and supporting directives.

5.3.2. The security accreditation process shall include the following aspects:

- (a) the scope and purpose of the security accreditation process, including National/NATO security policies to be followed;
- (b) the description of the CIS, including resource and activities planning/scheduling and interconnectivity requirements;
- (c) the responsibilities of the authorities/personnel involved in the security accreditation process (e.g. NATO/National SAA, CISPIA, CISP, CISOA and project staff);
- (d) the specific items of evidence (e.g. results of the security implementation verification) that will be required, and the assessment process to be followed in order to reach a security accreditation decision, as defined in the SAP;
- (e) the processes for ensuring the security accreditation of the CIS throughout its operational life-cycle.

5.4. Approval for testing

5.4.1. When there is a requirement to test the CIS before this is used in its final operational environment, the SAA may grant an Approval for Testing (AfT) by identifying specific conditions for the AfT including, for example, the scope of the CIS to be tested, the classification of information involved in the testing, the test plan and the timeframe for the AfT.

5.5. Security Accreditation Outcome

5.5.1. After following the activities involved in reaching a security accreditation decision, the SAA has a number of options, as follows:

- (a) issuing a Security Accreditation Statement (SASSt) for a specified period of time for the planned operational environment, where all security requirements are met; a SASSt shall always state the conditions for the security accreditation to remain valid. The validity of a security accreditation shall not exceed 36 months;
- (b) issuing an Interim Security Accreditation Statement (ISASSt) for a specified period of time for the planned operational environment, where not all security requirements are met. The statement shall clearly identify the conditions for the ISASSt (e.g. mitigating measures or reduced functionalities), the activities to be undertaken and completed to achieve transition from ISASSt to SASSt (e.g. final approval of security-related documentation), and the timeframe for the ISASSt;
- (c) denying security accreditation; this implies identifying specific deficiencies and corrective actions;
- (d) revoking an existing security accreditation; this implies identifying specific deficiencies and corrective actions.

5.6. Ongoing Security Accreditation Activities

5.6.1. The SAA shall continue to oversee the security arrangements for the CIS under its responsibility, primarily by ensuring periodic re-assessments of the security risks, where appropriate, and periodic security audits (e.g. inspections, reviews) of the security arrangements in place, in accordance with the requirements of NATO security policy and supporting directives.

5.6.2. It is the responsibility of the CISPIA, CISP and CISOA to inform the SAA 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 handled. The SAA shall advise on any security implications of any of the proposed changes.

5.6.3. The security re-accreditation conditions shall be clearly stated in the security-related documentation for a CIS or in a CIS-specific security accreditation process. In order to identify the requirements for re-accreditation of a CIS, the SAA should consider the extent to which the CIS and its security/operational environment have changed.

6. Security Risk Management for NATO CIS

6.1. General

6.1.1. NATO policy requires that NATO CIS be subject to security risk management. The principles and application of security risk management may also be adopted by national SAA for national systems handling NATO classified information.

6.1.2. Security risk assessment is the process of identifying security risks⁶, i.e. the threats and vulnerabilities of a CIS, determining their magnitude and identifying areas needing countermeasures. Security risk assessment serves to identify the risks that exist, identify the current security posture of the CIS in respect to handling information, and then assemble the information necessary for the selection of effective security countermeasures, based upon NATO security policy and supporting directives and guidance.

6.1.3. 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 staff.

6.1.4. 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 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.

6.1.5. 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.

6.1.6. 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.

⁶ For the purpose of this Directive, Security Risk is defined as the likelihood of a CIS's inherent vulnerability being exploited by the threats, leading to the CIS and/or the information handled being compromised.

6.1.7. 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.

6.1.8. 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 CIS Security measures.

6.1.9. 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.

6.1.10. 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.

6.2. The Security Risk Assessment and Risk Management Processes

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

- (a) what assets are at risk;
- (b) what is the impact or consequence if the identified vulnerabilities are exploited successfully.

6.2.2. The security risk assessment and risk management processes shall be undertaken jointly by the CISPIA, the CISOA, the CISP and the SAA. The security risk assessment and risk management processes shall follow a structured approach (either carried out manually or using an automated tool).

6.2.3. The security risk assessment process shall include the following stages:

- (a) identification of the scope and objective of the security risk assessment; the objective shall be agreed between the CISPIA, the CISOA, the CISP and the SAA;

- (b) determination of the physical, personnel and information assets which contribute to the fulfilment of the mission of a CIS or an organisation's mission;
- (c) determination of the value of the physical and personnel 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 their level;
- (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.

6.2.4. The security risk management process shall include the following stages:

- (a) 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:
 - i. risk avoidance – the objective being to eliminate the risk by removing the activity or changing the condition that gives rise to the particular risk;
 - ii. risk mitigation – the objective being to implement countermeasures to the extent that the risk is limited to an acceptable level;
 - iii. risk acceptance – the objective being a decision 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;
- (b) 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.

6.2.5. The security risk management process can provide the details to be included in the security-related documentation required in the NATO security accreditation

process. The outputs of the security risk management process shall be approved by the SAA, in coordination with the CISOA. The residual risk shall be subject to the approval of the CISOA.

6.2.6. The security risk management process is also the foundation for developing business continuity requirements. 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.

6.3. On-going Security Risk Management

6.3.1. 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 SAA or as stated in an agreed security accreditation process.

7. Security-Related Documentation

7.1. General

7.1.1. This section deals with the security-related documentation requirements, in support of the security accreditation process. The security-related documentation defines the scope, security requirements, security environments and security measures of the CIS to be security accredited. It also identifies the management responsibilities and authority of the entities (e.g. CISPIA, CISP, CISOA and SAA) involved in the security accreditation process.

7.2. Operational requirements for NATO CIS

7.2.1. Operational requirements for NATO CIS are captured in formal documents (e.g. Capability Packages) which are utilised as a major part of the acquisition process. NATO documents relevant to the acquisition of CIS shall address, coordinated by the appropriate CISPIA, CISP, CISOA and SAA, the required NATO CIS Security aspects, including security accreditation resources (e.g. funding/manpower for risk and vulnerability assessment).

7.3. Security Risk Management Report for NATO CIS

7.3.1. Paragraph 6.2.4 of this directive addresses the requirement for a Security Risk Management Report.

7.4. Security Architecture for NATO CIS

7.4.1. A security architecture is developed to create a chain of traceability between the business objectives and the security measures to be implemented in a CIS. A security architecture is also essential to understand how the security measures planned for a CIS integrate and complement each other and how they contribute to the overall security of the CIS.

7.4.2. When a security architecture is being developed for NATO CIS, this shall be checked against existing reference security architecture(s) to ensure security coherence and integration of new CIS in existing infrastructure(s).

7.5. Security Accreditation Plan/Security Accreditation Strategy

7.5.1. For all NATO CIS and other CIS handling NATO classified information the CISPIA shall develop a SAP or national equivalent to describe the steps to be taken to achieve security accreditation respectively of a CIS or of a set of CIS under the authority of an SAA. The SAP shall be approved by the relevant SAA.

7.5.2. The SAP shall contain information about the planned CIS, the authorities involved in the security accreditation process, the activities to be performed (possibly including their security accreditation schedule to accommodate resources) and the documentation to be produced.

7.5.3. An SAS can be developed by an SAA to provide common direction on how to accredit a set of CIS under its authority, by establishing goals, defining tasks and processes as well as identifying responsibilities and resources.

7.6. Security Requirement Statements

7.6.1. For all NATO CIS and other CIS handling NATO classified information, the security requirements shall be formulated and formally captured by the appropriate CISPIA as well as approved by the SAA.

7.6.2. For NATO CIS the security requirements shall be incorporated in the form of a Security Requirement Statement (SRS). For National CIS handling NATO classified information, national equivalent means may be used to formally set security requirements.

7.6.3. The SRS (or national equivalent) 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.

7.6.4. The SRS (or national equivalent) 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. The SRS is also affected 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 and user requirements.

7.6.5. The SRS (or national equivalent) forms an integral part of the user and operational requirement. In its final form, the SRS (or national equivalent) constitutes a complete statement of what it means for the CIS to be secure.

7.6.6. The SRS (or national equivalent) specifies how security is to be achieved, managed and checked. It forms the binding agreement between the CISP and the SAA, and constitutes part of the security accreditation process.

7.7. Role of an SRS

7.7.1. The following outlines, in general terms, the role of the SRS (or national equivalent) 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 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), as agreed with the appropriate SAA, 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) 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 accreditation - the SRS (or national equivalent) shall form the basis for the formulation of SecOPs (or national equivalent), specifying the procedures that are to be implemented to secure the CIS. Before a CIS goes into live operation, the SRS (or national equivalent), supported by the remaining evidence required by the security accreditation process, shall form the basis for security accreditation;

- (d) CIS operation/enhancement – the SRS (or national equivalent) shall form the basis of an understanding between the CISP and the appropriate SAA that the CIS is intended to operate in a secure manner. It defines the demarcation line between the security responsibilities devolved to the security management staff and those resting with the appropriate SAA and other security staff with jurisdiction in the same Global Security Environment⁷/Local Security Environment⁸. The SRS (or national equivalent) is to be maintained under rigorous configuration control by the CISP over the CIS life-cycle and any changes made should be undertaken in conjunction with the SAA. The SRS (or national equivalent) is used as a reference point in security audits and in any security 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;
- (e) CIS withdrawal from service/disposal of equipment - the SRS (or national equivalent) 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.

7.8. Types of SRS

7.8.1. For NATO CIS the SRS shall 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 shall be formulated. This is to be supported by individual SSRs for each of the interconnected CIS. In addition, this should facilitate the aggregation of a series of bilateral System Interconnection Security Requirement Statements (SISRSs), 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 CISP and different SAA, the CSRS review and approval processes may be undertaken by a number of co-ordinating SAAs.

The CSRS may also be used to cover a community of CIS in a large organisation (e.g. NATO HQs, SCs, 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,

⁷ The physical security measures surrounding the location where the system is installed (e.g. perimeter / building security).

⁸ The non-CIS Security measures (e.g. personnel, information, physical) surrounding the office areas where components of system are located (e.g. server rooms, user workstation areas, network communication areas).

the CSRS review and approval process shall be carried out by the organisation's SAA;

- (b) System-specific Security Requirement Statement (SSRS) - in elementary situations (e.g. small stand-alone information systems), the only SRS that may be required by the SAA is an outline SSRS. In more complex cases (e.g. large local area networks), where a more comprehensive statement is required, the SSRS should evolve during the project life-cycle and shall be approved by the SAA as part of the security accreditation process;
- (c) System Interconnection Security Requirement Statement (SISRS) – when two CIS are required to be interconnected to exchange information, an SISRS is required to be formulated, which forms the basis of a security agreement between the relevant CISP and SAA.

7.8.2. The types of SRS (or national equivalent) necessary in any given circumstance is determined by the SAA, in conjunction with the CISPIA and CISP.

7.9. Security Test and Verification Plan and Report

7.9.1. A Security Test and Verification (ST&V) Plan (or national equivalent) is a description of the security testing and verification of the CIS Security measures to be implemented.

7.9.2. For each security-relevant or security-enforcing CIS Security function, as determined by the SAA, 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;
- (d) the pass criteria for the security test;
- (e) the results of the security test.

7.9.3. The ST&V requirements necessary in any given circumstance is determined by the SAA, in conjunction with the CISPIA and the CISP. The SAA shall be responsible for approving the ST&V Plan (or national equivalent), and the results of the security testing which shall be provided in the form of a ST&V Report (or national equivalent), as part of security accreditation process.

7.10. Security Operating Procedures

7.10.1 Security Operating Procedures (SecOPs) (or national equivalent) are a description of the implementation of the security measures to be adopted, the operating procedures to be followed and the responsibilities of the personnel. SecOPs shall differentiate between the security requirements for the CIS users and those performing security management as well as administrative functions.

7.10.2 The SecOPs (or national equivalent) shall be prepared by the CISP, in consultation with the CISPIA and the SAA. The SAA shall approve the SecOPs (or national equivalent), as part of the security accreditation process of any NATO CIS or any other CIS handling NATO classified information.

7.10.3 The following sections are required to be addressed in the SecOPs (or national equivalent), as a minimum:

- (a) administration and organisation of security, including points of contact;
- (b) personnel security, physical security, security of information;
- (c) CIS Security;
- (d) Incident and emergency procedures;
- (e) configuration management;
- (f) acceptable use policy.

8 Security Accreditation of the Interconnection of NATO CIS

8.1 This section identifies and mandates the security accreditation requirements for interconnecting NATO CIS with other CIS (e.g. 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).

8.2 The principles of security risk management, minimality, least privilege, self-protecting CIS, defence-in-depth, up-to-date security posture, resilience, security functionality assurance and security compliance shall be applied when connecting NATO CIS to the other CIS identified in the paragraph above, as required by the Primary Directive on CIS Security.

8.3 The SAA, in co-ordination with the appropriate CISPIA and CISP, shall:

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

- (b) approve the security risk assessment/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 as well as the on-going security risk management processes;
- (d) establish the requirement for security-related documentation;
- (e) review and approve the required security-related documentation;
- (f) approve the mechanisms and/or procedures for ensuring that the security objectives established for the CIS are met;
- (g) establish the requirements for ST&V and security audits;
- (h) approve the ST&V plan;
- (i) review the results of ST&V and security audit, and identify, where appropriate, any additional countermeasures to be implemented;
- (j) provide a security accreditation statement for the interconnection and state the conditions for security re-accreditation.

9 Assured CIS and security enforcing products

9.1 General

9.1.1 The Primary Directive on CIS Security requires that security functionalities of NATO CIS and other CIS handling NATO classified information as well as related security enforcing products shall be assured by trusted authorities through formal assurance techniques. These techniques are defined in the Primary Directive on CIS Security and include evaluation and security accreditation for CIS as well as evaluation, certification and approval for security enforcing products.

9.2 Evaluation and security accreditation for CIS

9.2.1 All NATO CIS and other CIS handling NATO classified information shall be subject to a security accreditation process to determine that an adequate level of protection has been achieved and is being maintained for a CIS. Security accreditation shall be supported by the results of an evaluation by, or under the control of, the appropriate national or NATO authority (e.g. SAA) to confirm that the CIS satisfies its pre-defined security requirements. The evaluation is based on the review of the security-related documentation, the findings of the ST&V and, when required by the SAA, of the security audit results (Type 3, 4 or 5 as defined in paragraph 11.2). For

NATO CIS, the evaluation shall also be based on the risk assessment outcome and, where appropriate, the security architecture.

9.3 Evaluation, certification and approval of security enforcing products

9.3.1 The evaluation of a security enforcing product is a detailed technical examination, by or for the appropriate national, international or NATO Evaluation Authority or its nominated competent representatives, 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. The aim of evaluation is to assemble evidence to allow for a certification and/or approval of a product.

9.3.2 The certification of a security enforcing product is the issue, by an appropriate national, international or NATO certification authority, of a formal statement, as a result of a successful evaluation.

9.3.3 Certification is carried out by the certifiers once in receipt of the evaluation reports. The certification process should include the following aspects and, shall be subject to national, international or NATO endorsement of the certification scheme:

- (a) resources for the evaluation - how much resource (e.g. time, 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.

9.3.4 The certification process normally results in the production of certification reports which state to what extent the product 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.

9.3.5 The approval of a security enforcing product is a formal statement, by a National CIS Security Authority (NCSA)⁹, 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. The approval of a security enforcing product for a CIS is a two-step process: while the approval by an NCSA is required to declare the product suitable for the protection of NATO information, the approval by an SAA is related to its use in the context of a specific CIS, as part of the security accreditation process.

9.3.6 For NATO CIS, the requirements for product evaluation, certification and/or approval shall be identified during the security accreditation process of a CIS in accordance with the following steps:

- (a) The CISOA defines the operational requirements;
- (b) The CISPIA, in coordination with the CISOA and SAA, undertakes a security risk assessment;
- (c) Where appropriate, the CISPIA develops a security architecture based on the mission objectives, the findings of the security risk assessment and the minimum security requirements set in the NATO security policies and supporting directives;
- (d) The CISPIA shall identify the security functions required by the security architecture and the security enforcing products which could provide such functions;
- (e) Security enforcing products in the categories of cryptographic equipment, emission security related equipment (TEMPEST), operating systems and equivalent platforms (e.g. firmware), and border protection equipment (e.g. firewall and application gateways) shall be approved by an NCSA;
- (f) As result of the security accreditation process, the SAA may request an NCSA approval of products not included in the categories listed above;
- (g) The NCSA approval shall be based on the NATO agreed evaluation and certification scheme or national equivalent, and in accordance with the provisions of Enclosure "F" of the Policy on Security within the North

⁹ or other competent national authority

Atlantic Treaty Organisation and relevant technical and implementation directives and supporting documents on CIS Security;

- (h) The use of security enforcing products in a CIS has to be finally approved by the SAA, as part of the security accreditation process, based on the development of specific security configuration/baselines for the product and on the successful execution of security testing (e.g. ST&V, vulnerability assessment) by the CISP.

9.3.7 For other CIS handling NATO classified information, the requirements for product evaluation, certification and/or approval shall be identified during the security accreditation process of a CIS in accordance with the steps at paragraphs 9.3.6 (e), (f), (g) and (h).

9.3.8 The CISPIA should primarily refer to the NATO Information Assurance Product Catalogue which lists the products which have been endorsed specifically for the protection of NATO information.

10 Management of Security Implementation of CIS

10.1 General

10.1.1 This section deals with the requirements for the management of the security implementation of NATO CIS and other CIS handling NATO classified information.

10.1.2 Managing the security implementation of a CIS, once this is security accredited, requires ensuring that any change (intentional and unintentional) affecting the security posture of the CIS is properly addressed throughout its operational life. The objective is to ensure that the CIS continues to be conformant with NATO security policy and supporting directives, and the CIS-specific SRS (or national equivalent).

10.2 Security Implementation Management Requirements

10.2.1 For all NATO CIS and other CIS handling NATO classified information, the CISP shall establish control procedures to ensure that all CIS changes are reviewed for their security implications.

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

10.2.3. All NATO CIS and other CIS handling NATO classified information shall be subject to security management through the use of appropriate security tools. For NATO CIS, CISP shall maximise the use of automated tools to continuously assess

CIS compliance to security baselines. The security tools shall be subject to the approval of the SAA, in conjunction with the CISPIA and CISP.

10.2.4 The SAA, in conjunction with the CISPIA, CISOA and CISP, shall establish the requirements for the use of security tools to perform the following activities:

- (a) identification and prevention of unauthorised activities having a potential impact on the security objectives of the CIS;
- (b) intrusion detection/prevention – 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 paragraph 11.2 of this directive;
- (d) security configuration checks – to ensure that the configuration is established and maintained in its approved state, in accordance with the requirements of the security-related documentation and the security baselines defined by the CISP, in conjunction with the SAA.

10.2.5 The SAA shall establish the requirements, in conjunction with the CISOA, CISPIA and CISP, on how to report security violations.

11 Security Audit of CIS

11.1 General

11.1.1 A security audit is a systematic review of a CIS in order to ascertain its susceptibility to compromise of the security objectives. A security audit can determine the susceptibility of a CIS to a specific attack, or determine the opportunity to a threat agent to exploit vulnerabilities. A security audit can be undertaken either as part of an on-going security risk management process or as part of the on-going security accreditation process.

11.2 Types of Security Audits

11.2.1 A Type 1 security audit is a documentation review addressing the services provided by the CIS and the overall CIS architecture. The CIS architecture is analysed to determine compliance to the requirements of the NATO security policy and the security baselines defined by the CISP as well as to identify potential access points and paths for an adversary to attack CIS assets.

11.2.2 A Type 2 security audit is the periodic security inspection carried out by the SAA, resulting in the production of a formal report that is provided to the head of the organisation. The Type 2 security audit involves:

- (a) the review of security-related documentation;
- (b) review of configuration management;
- (c) interviews with management, security management staff and users;
- (d) site inspection of the personnel security, physical security, security of information, and CIS Security measures in place.

11.2.3 In circumstances where the risk is low, the results of the previous inspections are positive and manpower and expertise are available at the CISOA, the SAA may consider authorising the head of the organisation, acting as CISOA, to carry out a self-inspection in conjunction with the CISP. In this case the inspection report shall be signed by the head of the organisation and sent to the SAA. Once exercised, a self-inspection shall be followed by a regular security inspection within a period of 12 months.

11.2.4 A Type 3 security audit is the vulnerability assessment carried out by the CISP (or by a competent NATO (e.g. SECAN) or National authority), in coordination with the CISOA and the SAA. It complements Type 2 security audits by using security tools to map the CIS, test the system and network components for security weaknesses, and check the system management software for completeness. A report of the vulnerabilities is produced, together with recommendations to resolve them.

11.2.5 A Type 4 security audit is carried out by a team independent from the CISP (a competent NATO or National authority) and complements Type 2 and 3 security audits. The independent team actively attacks the CIS to exploit any weaknesses, using security tools (e.g. network and host vulnerability scanners, network and host exploitation tools, monitoring tools). A Type 4 security audit is carried out with the prior approval of the CISOA, the CISP and the SAA. A Type 4 security audit is carried out with the full knowledge and close co-operation of the CISP (including CIS administrators).

11.2.6 A Type 5 security audit is conducted accordingly to the requirements of the Type 4 with the difference that this is performed without the full knowledge and close co-operation of the CISP. In any case the prior approval of the CISOA, the Head of the CISP and the SAA is required.

11.2.7 The use of third-party partners (e.g. industry, governmental entities) to perform or support the execution of security audits shall be subject to the consent of the SAA, after appropriate consultation with the competent NATO or National authority, as appropriate.

11.3 Security Audit Requirements

11.3.1 All NATO CIS and other CIS handling NATO classified information shall be subject to security audit on a periodic basis under the authority of the SAA.

11.3.2 The SAA shall, in conjunction with the CISOA and the CISP, determine the requirement for security audits either as part of an on-going security risk management process or as part of the on-going security oversight or security accreditation process. Where a requirement is established, the SAA shall agree the mechanisms and procedures, and shall review the results of the security audits in order to determine whether additional security countermeasures are to be implemented.

11.3.3 In order to maximise effectiveness and efficiency of efforts, any activity conducted by the CISOA and the CISP to verify the security implementation of CIS shall be appropriately coordinated with the SAA.

11.3.4 The SAA shall consider whether specific inspection frequency schedules are explicitly imposed by other NATO security policies and directives on critical assets (e.g. COSMIC TOP SECRET, ATOMAL, NATO Public Key Infrastructure).

11.3.5 The scope of all security audits shall be clearly established and documented.

11.3.6 For Type 3, 4 and 5 security audits, the security rules of engagement, including responsibilities, procedures, methodologies and techniques, shall be clearly identified and documented as well as subject to National and NATO legal requirements.

11.3.7 For all security audits, 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 CISOA, the CISP and the SAA.

Appendix 1 - General CIS Security Aspects**1. Handling and Control of Removable Computer Storage Media**

1.1. All removable computer storage media holding NATO classified information are documents 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.

1.2. 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 laws 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);
- (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.

1.3. For NATO civil and military bodies, as part of security risk management, controls may be mandated by the SAA for media holding information bearing other security classification markings.

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

2.1. 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.

2.2. 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.

3. Security During Processing

3.1. 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.

3.2. Release of information classified NATO CONFIDENTIAL and above to unmanned facilities shall be prohibited unless special arrangements approved by the SAA are in force and have been specified in the security-related documentation.

4. Use of Privately-Owned Equipment for Official NATO Work

4.1. 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 NATO classified information.

4.2. 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.

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

5.1. 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 SAA shall security accredit the system.