NORTH ATLANTIC COUNCIL

CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

11 November 2024

DOCUMENT
AC/35-D/2004-REV4

SECURITY COMMITTEE

Primary Directive on CIS Security

Note by the Chair

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

2. This directive, approved by the Security Committee (SC) in CIS Security (CISS) format under silence procedure, will be subject to periodic reviews.

3. This document supersedes AC/35-D/2004-REV3 with the exception of Appendix 2 "CIS Security-related Activities in the CIS Life Cycle" which remains in force until further notice.

4. This Directive also replaces Section 4 "CIS Security Roles and Responsibilities" of the Management Directive on CIS Security (ref. AC/35-D/2005-REV3) with immediate effect.

(signed) Galen J. Nace

Annexes: 1
Appendixes: 4

Action officer: V. Virili, JISD/NOS/SPOB/CSS, ext. 3506
Original: English

ANNEX 1
AC/35-D/2004-REV4

Primary Directive on CIS Security

Contents

1. Introduction

1.1. The requirement to protect NATO Information, supporting systems, 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 and directives:

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

b) Security within the North Atlantic Treaty Organization (NATO) (C-M(2002)49-REV1);

c) Protection of NATO Civil and Military bodies (C-M(2002)50-REV1)[1];

d) Management of Non-Classified Information (C-M(2002)60);

e) NATO Comprehensive Cyber Defence Policy (PO(2021)0199); and

f) Directive on the Protection of Communication and Information Systems (CIS) Handling Non-Classified NATO Information (AC/35-D/2020).

1.2. In particular, Enclosure “F” of the NATO Security Policy 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[2] in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

2. Purpose

2.1. The Primary Directive on CIS Security[3] is published by the Security Committee (SC) for the following purpose:

a) to support the implementation of the NIMP, Enclosure "F" of the NATO Security Policy, and the NATO Comprehensive Cyber Defence Policy;

b) to provide the relation among the NIMP, the NATO Security Policy, the NATO Comprehensive Cyber Defence Policy, the CIS Security Management Directives and guidance published by the SC, and the CIS Security Technical and Implementation Directives and guidance published by the Digital Policy Committee (DPC)[4];

c) to set out CIS Security activities in the life cycle of CIS which are essential to identify an appropriate level of protection for CIS handling NATO Information to cope with

---

1 In the scope of this Directive, references b and c are jointly referred to as “NATO Security Policy”.

2 Within this Directive ‘stored, processed, or transmitted’ is also referred to as “handled”.

3 For NATO bodies, the term “CIS Security” shall be considered as identical to “Cyber Security” (ref. AC/322-N(2019)0043-REV1). While the former should be preferred, their use is interchangeable for all intents and purposes (as an example, the role of a Cyber Security Officer shall be considered as identical as the one of a CIS Security Officer). This equivalence is extended to all those Nations that have regulated the term cyber security accordingly in their legislative framework.

4 Formerly known as Consultation, Command and Control Board (C3B).

the evolving threat environment and enable organisations that fall under the scope of this Directive to securely fulfil their mission[5] objectives;

d) to identify NATO committees, national bodies, NATO Civil and Military bodies, and NATO entities, with a key responsibility for CIS Security.

2.2. This Directive shall be complemented by a Directive on the Security Accreditation and Auditing of CIS, and supported by various technical and implementation directives, as well as supporting documents and guidelines on CIS Security, as published by the SC and the DPC.

3. Scope

3.1. This Directive is mandatory for all NATO Civil and Military bodies, NATO Nations, and Non-NATO Entities (NNE) that own, procure, design, implement, operate, or support CIS handling NATO Classified Information.

3.2. For NATO Civil and Military bodies, the applicability of this Directive also extends to NATO CIS handling non-classified NATO Information. Additionally, in accordance with the Directive on the Protection of CIS Handling Non-Classified NATO Information, the scope of this Directive also includes CIS that are under national/multinational responsibility for their cyber defence but are used by organisations that have a formal arrangement with a NATO body (e.g. NATO Centres of Excellence (CoEs) and Memorandum of Understanding (MoU) bodies).

3.3. In situations where the boundaries of a CIS handling NATO Information include multiple entities (e.g. a NATO CIS provided or extended to a national entity, or vice versa), a shared responsibility model shall be formalised amongst the parties to ensure security responsibilities are delineated and security requirements are met, in compliance with this Directive.

3.4. National Security Authorities (NSAs), Designated Security Authorities (DSAs), Strategic Commands Security Authorities, and the NATO Office of Security (NOS)[6] are responsible for ensuring the implementation of this Directive and for providing independent recommendations, direction, and guidance on all relevant CIS Security matters.

3.5. In the context of the NATO Enterprise[7], the NATO Office of the Chief Information Officer (OCIO), in its role of Single Point of Authority on Cyber Security, shall enable a consistent and coherent implementation of this Directive for the entire NATO Enterprise, including a mature enterprise-wide management of Cyber Security risks and the setting of cyber requirements for both civilian and military stakeholders. The OCIO shall also act as the NATO Enterprise CIS Operational Authority (CISOA), as further described in Sections 6.2 and Appendix 1 of this Directive.

---

5 The term mission throughout this Directive includes “NATO operations, projects, programmes, contracts and other related tasks”, ref. NATO Information Management Policy (C-M(2007)0118), and is not limited to those NATO missions which might be considered only military in nature.

6 The NATO Office of Security and the Strategic Commands Security Authorities are collectively referred to “NATO Security Authorities” with their specific roles and responsibilities being already identified in the Policy on Security within NATO (ref.: C-M(2002)49-REV1) and its supporting directives.

7 Hereafter the term ‘NATO Enterprise’ refers to all NATO Civil and Military bodies, and relevant NATO CIS, that fall in the scope of the NATO Enterprise approach, as defined by the DPC.

4. CIS Security Frameworks

4.1. The definition of security requirements to protect CIS that fall under the scope of this Directive shall follow a structured approach to ensure security activities are executed throughout the entire life cycle of a CIS and can ultimately enable the organisation to securely fulfil its mission requirements.

4.2. A CIS Security Framework shall be defined and developed to support organisations in executing these security activities in a coordinated, measurable, and standardised form. The main objective is to ensure CIS Security risks affecting the organisation and its systems can be identified, measured and treated accordingly.

4.3. The following four security pillars shall be considered during the development of any CIS Security Framework meant to protect CIS that fall in the scope of this Directive:

- A CIS Security Management System: Set of CIS Security roles, processes, procedures, and activities that shall be in place in the organisation and sufficiently resourced to ensure compliance with the relevant NATO Security Policy requirements and enable the management and monitoring of security risks affecting CIS and the information they handle;
- Security-by-Design: Set of security principles and technical measures that shall be respectively followed by the organisation and implemented within the CIS, since the earliest stages of its life cycle, to ensure its security posture is adequate to cope with the existing and anticipated threat landscape;
- Security Operations: Set of security activities to support the secure operations of CIS and their components with the aim of maintaining over time, and if required also improving, an effective and resilient security posture of the CIS;
- Security Objectives: To enable the organisation in achieving its missions and in maintaining Information Superiority[8], NATO Information handled in the CIS[9] shall be protected with respect to its confidentiality, integrity, availability, non-repudiation, and authentication requirements.

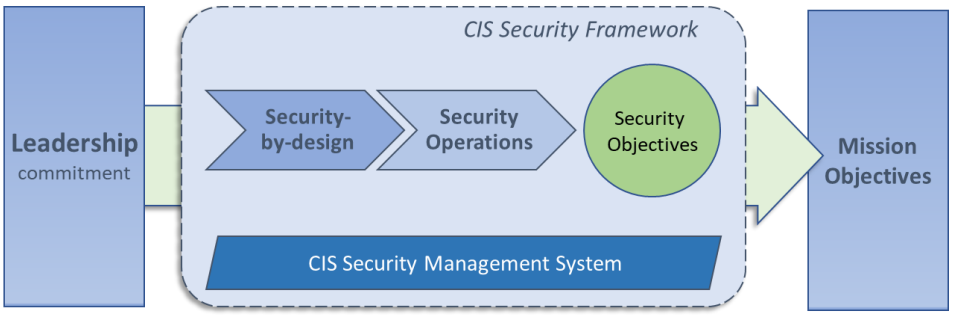

Figure 1 – Representative example of a CIS Security Framework

8 Def. “State of relative advantage in the information domain achieved by getting the right information to the right people at the right time in the right form whilst denying an adversary the ability to do the same.”

9 In accordance with C-M(2002)49-Rev1, NATO Nations are responsible to protect and safeguard NATO Classified Information. Nevertheless, in line with The Primary Directive on Information Management (ref. C-M(2008)0113), NATO Nations are recommended to apply the same CIS Security Objectives for the secure handling and protection of non-classified NATO information.

4.4. Fundamental to the success of any implementation of a CIS Security Framework, including its alignment with the organisation's mission, is the active involvement and commitment of the organisation's leadership.

4.5. Specifically, the Head of each body is responsible for the correct implementation and execution of the relevant CIS Security Framework and the required security activities.

4.6. These security activities shall be resourced, prioritised (in accordance with the security risk management principle), properly supported, and led by competent CIS security management staff which shall possess professional qualifications in the field of CIS Security, with adequate training and experience.

4.7. To protect CIS that fall under the scope of this Directive, the Head of the organisation shall ensure sufficient support to the security management staff in performing the following functions:

a) implementing and monitoring the execution of a CIS Security Framework within their organisation;

b) in NATO bodies, implementing the NATO Security Risk Management Process (NSRMP)[10] for security risks affecting NATO CIS and ensuring these risks are properly managed, to include their identification, treatment, monitoring, and required reporting;

c) ensuring the correct implementation and maintenance of required security 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;

d) ensuring security activities and processes are embedded in the life cycle of any CIS, from its initial design, during its operations and until its full decommissioning. This includes, but is not limited to, ensuring the security accreditation process is followed for any CIS to guarantee that these achieve and maintain an appropriate and approved security posture;

e) defining and implementing CIS Security incident response requirements and processes to ensure prompt detection and responses to security incidents affecting the organisation;

f) promoting a security culture across the organisation by delivering security education and awareness sessions to all staff in the organisation and tailored to their job position;

g) supporting the definition and implementation of a Business Continuity Plan (BCP) in line with requirements coming from leadership and other business stakeholders;

h) ensuring that security audits are conducted regularly to verify that CIS Security measures are implemented and maintained in accordance with the NATO Security Policy and its supporting directives;

i) ensuring compliance with all relevant security requirements applicable to a given CIS, as stemming from the NATO Security Policy and its supporting directives; and

[10] Reference "NATO Security Risk Management Process (NSRMP), AC/35-D/1035".

j) assessing the effectiveness and efficiency of security-related activities within the organisation and ensuring these are improved should gaps be identified (e.g. corrective actions, deficiencies, observations, and recommendations).

5. Security Objectives

5.1. Enclosure “F” of the NATO Security Policy and the Directive on the Protection of CIS Handling Non-Classified NATO Information each sets the following five security objectives respectively for information which is NATO classified and for information which is NATO non-classified:

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

b) integrity - to ensure the integrity of NATO Information and supporting systems, services, and resources;

c) availability - to ensure the availability of NATO Information and supporting systems, services, and resources;

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

e) non-repudiation - to ensure appropriate non-repudiation for individuals and entities having processed the information[11].

5.2. The degree of applicability of these security objectives is specific to any CIS and shall be determined during the security accreditation process considering a number of factors including the mission objectives, the minimum security requirements established by the NATO Security Policy, the Directive on the Protection of CIS Handling Non-Classified NATO Information, and the results of the security risk management process.

[11] This objective may require the generation and protection of indisputable proof for claims made by, or for, individuals and resources accessing, distributing, or receiving NATO information.

6. CIS Security Management System

6.1. CIS Security Management System Overview

6.1.1. To ensure security-related activities can protect NATO Information while actively enabling the organisation in executing its mission, a set of security management roles, processes and procedures shall be defined and implemented with the support of the organisation's leadership.

6.1.2. In detail, the purpose of the CIS Security Management System is to lay down the foundations that shall enable the organisation to accomplish its mission, while ensuring security compliance and an acceptable residual security risk are achieved and can be maintained.

6.1.3. Each organisation, shall draw up the necessary implementation regulations to ensure compliance with the NATO Security Policy, its supporting directives and, for NATO bodies, also the CIS Security Framework described in this document. Internal security regulations of NATO bodies shall be endorsed by the relevant NATO Security Authority with the OCIO ensuring a coherent and homogenous approach to CIS Security across the NATO Enterprise.

6.2. Roles and Responsibilities

6.2.1. As introduced in section 4, the Head of any organisation falling in the scope of this Directive is ultimately responsible and accountable for any action and decision taken in their organisation and, for NATO bodies, they are also the security risk acceptance authority within their area of responsibility. As a result, the Head of the organisation shall appoint qualified staff[12] to support them in the execution of their responsibilities of local security authority and business/risk owner, while maintaining adequate separation between these two functions to avoid conflicts of interest.

6.2.2. This requires, on the one hand, the formalisation of the security roles and relevant job positions by defining a 'security organisation'. Such organisation shall include at least one Security Officer (SO)[13] and one CIS Security Officer (CISSO), the latter being responsible for the security oversight of all CIS Security aspects within the organisation. Depending on the context the organisation operates in, mission objectives, and in coordination with the relevant Security Authority, leadership may assign all security roles and responsibilities in the security organisation to one individual.

6.2.3. On the other hand, and complementing the above, a CISOA shall be functionally established within the organisation to represent the business in terms of requirements for new and existing CIS capabilities, to correctly implement this Directive, to ensure CIS that fall under the scope of this Directive are security accredited before authorising their operations and, for NATO bodies, to manage security risks throughout the life cycle of relevant NATO CIS.

---

12 Qualified staff refers to staff who has the management and technical experience and capability to support the Head of the organisation.

13 Ref. Section 3, "Basic Principles" of C-M(2002)50-REV1.

CIS Security Officer (CISSO)

6.2.4. The security oversight responsibilities of a CISSO include, but are not limited to:

a) ensuring their organisation correctly implements the NATO Security Policy and its supporting directives with respect to CIS Security requirements;

b) providing CIS Security advice to the organisation's leadership and other stakeholders, as well as maintain the required CIS Security awareness within the organisation;

c) ensuring a record of all persons authorised to use any part of the CIS is maintained together with the extent of their authorisation and ensure that those persons have the Personnel Security Clearance, where required, and need-to-know for the information handled in the CIS, in accordance with the CIS mode of operations;

d) overseeing, and initiating when necessary, the CIS change management process to ensure security is maintained during implementation and maintenance of hardware, firmware and software modifications and enhancements to the CIS. This includes ensuring that contractual agreements, for CIS hosted and/or operated by third-parties, contain the relevant security requirements that would allow such CIS to be managed and operated in accordance with the NATO Security Policy and its supporting directives;

e) ensuring the organisation correctly applies transmission, cryptographic, and emission security provisions, including the handling, maintenance and protection of cryptographic material, in accordance with the requirements of relevant NATO regulations[14];

f) ensuring security-related logs, including those related to event/process failure and authorised/unauthorised users' and system activities, are monitored and audited regularly. As required, to support the execution of their responsibilities, the CISSO shall be able to access security logs and associated monitoring and auditing tools;

g) conducting, coordinating, or supporting the execution of periodic security-related assessments of CIS (e.g. risk assessments, Security Testing & Verification (ST&V), security inspections, spot checks, vulnerability assessments, penetration tests, threat hunting, and other relevant security audits);

h) overseeing and advising on the definition, implementation, and regular testing of business continuity and disaster recovery requirements for the CIS in accordance with the objectives of the organisation's BCP;

i) ensuring Security Operating Procedures (SecOPs), or national equivalent are developed and maintained for the CIS in use by the organisation, and made available to their administrators and users who formally acknowledge that they will comply with them;

j) reporting regularly to the SAA on any detected CIS Security vulnerability and threat, as prescribed in the relevant SecOPs, and any deviation from approved documentation; and

[14] In some NATO regulations this role may be still referred to as "INFOSEC officer".

k) responding to and security investigating CIS Security incidents in line with the CIS security incident management procedures as endorsed by the relevant Security Authority. The response to CIS Security incidents shall be in close coordination with the security organisation (e.g. Security Officer), the local and enterprise CISOA (e.g. the OCIO for NATO bodies), the CIS Provider (CISP), the SAA and, where required, the technical incident responder (e.g. National Computer Emergency Response Team, NCI Agency / NATO CIS Security Centre) and the appropriate counter-intelligence authority. The CISSO shall also report the conclusions to the SAA, through the established management structure, and in line with the overall direction given by the relevant Security Authority.

6.2.5. Large or federated organisations using or operating complex or multiple CIS, may require the appointment of different CISSOs to ensure a sufficient and an effective CIS security oversight capacity across the whole organisation. In such circumstances, to ensure such oversight is coherent and comprehensive, a primary CISSO shall be appointed who may, subject to the endorsement of the relevant Security Authority and while maintaining a central security oversight, delegate the execution of some of their responsibilities to other individuals in the security organisation.

6.2.6. When such responsibilities are delegated to or supported by individuals outside the security organisation (e.g. CISOA, CISP, or a trusted industry provider), the delineation of these functions shall avoid conflict of interest and be formally agreed by all interested parties through legislative or policy governance. This includes Service Level Agreements (SLAs) or similar contractual arrangements, or internal security regulations that shall be endorsed by the relevant Security Authority.

6.2.7. Finally, the CISSO shall report directly to the Head of the security organisation and, when necessary, have direct or privileged access to the Head of their body in order to fully exercise their local security authority functions.

CIS Operational Authority (CISOA)

6.2.8. The CISOA, also known as the business/risk owner, plays an active and crucial role throughout the entire life cycle of a CIS and is specifically responsible for:

a) formally defining and managing business and operational requirements for new and existing CIS capabilities, their associated operating principles and concept of operation, including their information exchange requirements, and sponsor them when necessary both financially and administratively throughout the organisation;

b) ensuring all CIS-related projects and programmes in support of the business and mission requirements are compliant with NATO Security Policy, its supporting directives, and the specific requirements stemming from the Security by Design and CIS Security Operations pillars presented in this Directive. This includes ensuring that CIS Security requirements are included at the earliest phases of the capability development process and kept consistently and effectively operated;

c) liaising, where applicable, with the CIS Planning and Implementation Authority (CISPIA), the CISSO, 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;

d) accepting formally the residual security 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 NATO Security Policy, the CISOA shall not accept a level of risk higher than the that considered acceptable by the SAA through the approval of the security risk assessment[15];

e) ensuring that the SLAs or similar mechanisms, established with the CISP for the provision of CIS services, include the requirements for implementation, operation, monitoring and change management of security measures;

f) duly executing security-related projects and programmes to support and, where applicable, improve the security posture of the CIS;

g) conducting operational evaluation of the CIS and formally authorising the CIS for operational use, once the security accreditation is granted by the SAA[16], through the issuing of an authorisation to operate, or national equivalent;

h) informing the SAA on the status of their CIS and requesting security reaccreditation in accordance with the requirements of the security accreditation process;

i) acting as top-level CIS Security incident manager for the organisation by ensuring that such incidents can be prevented, detected, and responded upon. All responses shall be executed in coordination with the CISSO and SAA, in conjunction with the CISP, and by assessing the damage caused by the incident with the conclusions reported to the SAA;

j) ensuring the observation and alignment with the organisation's BCP and Disaster Recovery Plan (DRP) for the CIS under its responsibility; and

k) ensuring that contractors or other organisations designing, implementing, operating, and supporting the CIS have the appropriate security provisions in place, including the required need-to-know for the information they access.

CIS Planning and Implementation Authority (CISPIA)

6.2.9. Based on the business and operational requirements determined by the CISOAs, the CISPIA is responsible to design and implement the corresponding CIS, its functionalities, and the required security measures. For NATO CIS, this shall be accomplished also through the definition and use of security architectures, which will determine how security requirements can be implemented, following a risk-based approach, to meet both security and mission requirements, and associated funding arrangements, in line with extant NATO Security Policy and supporting directives.

6.2.10. In addition, the CISPIA is responsible for:

---

15 While the risk ownership and responsibility to accept and manage the security risks rest with the CISOA, the SAA shall confirm that the residual security risks are 'acceptable' from the perspective of being compliant with NATO Security Policy.

16 The Directive on Security Accreditation and Auditing of CIS examines the scenario where a given CIS has not been granted a Security Accreditation Statement, but NATO has an urgent and exceptional requirement to operate such CIS.

a) establishing the CIS Security technical and implementation aspects for CIS in conjunction with the CISP, relevant CISOAs, CISSO, project staff and the SAA;

b) ensuring that contractors or other organisations designing and implementing the CIS on its behalf have the appropriate security provisions in place, including the required need-to-know for the information they access;

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; and

e) defining the CIS Security resource requirements (e.g. staffing) in operational requirements for CIS.

CIS Provider (CISP)

6.2.11. The CISP is responsible for the security operations of a CIS throughout its life cycle and for its correct operation in line with mission requirements, associated funding arrangements, and security accreditation conditions.

6.2.12. More specifically, these responsibilities include:

a) formulating, and keeping under review, the security-related documentation required by the SAA with 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, CISSO 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) working with the CISSO and providing the required evidence to the SAA in order that security accreditation can be carried out in an effective manner;

f) operating and supporting the implemented CIS Security measures in accordance with the conditions of the given security accreditation and the approved SecOPs as well as responding to security incidents in a manner that is compliant with NATO Security Policy;

g) ensuring that contractors or other organisations operating, and supporting the CIS on its behalf have the appropriate security provisions in place, including the required need-to-know for the information they access;

h) maintain current Software Bill of Materials (SBOM), Firmware Bill of Materials (FBOM), and Hardware Bill of Materials (HBOM), for all CIS falling under its area of responsibility, in order to enable the management of those security risks and technical vulnerabilities that are introduced by supply chains;

i) checking, regularly 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; and

j) reporting regularly to the CISSO and CISOA any vulnerability found within the CIS or any deviation from approved documentation, in line with the requirements defined during the security accreditation process of the CIS and those determined by the CISSO and/or by the CISOA through agreed SLAs.

Security management staff – separation of duties

6.2.13. Security management staff is a generic category that includes those roles that perform CIS Security-related functions under the scope of this Directive. These roles include, among others, the CISSO, the staff supporting the work of the CISOA, security architects within the CISPIA, as well as CIS administrators, and crypto custodians working for the CISP. Segregation of duties shall be sought to avoid conflicts of interest amongst security management staff by requiring:

a) Adequate separation between the security organisation and the staff supporting the work of the CISOA, as delineated in paragraph 6.2.1;

b) Adequate separation to be maintained between the CIS administrators and the security organisation;

c) Further separation of duties amongst different CIS administrators (e.g. system, network, application, security) and CISP-internal security auditors; and

d) Overall, separation shall be duly considered and agreed with the relevant SAA at the earliest stages of the security accreditation process.

Security Accreditation Authority

6.2.14. As part of the security accreditation process of a CIS that falls under the scope of this Directive, the relevant SAA and all other authorities mentioned above shall be identified to ensure separation of duties and, for NATO CIS, a proper management of CIS Security risks through the life cycle of the CIS. Some of these roles may be played by the same organisational entity, however it is essential to maintain separation of duties between the SAA and all other roles.

6.2.15. The SAA is responsible for:

a) providing independent security advice, guidance, recommendations, and directions, in line with NATO Security Policy and its supporting directives, to all entities that fall in the scope of this Directive, relevant CISPIAs, CISPs, CISOAs, 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 associated interconnections. Where appropriate, these requirements should be captured in a Security Accreditation Strategy (SAS). The security accreditation processes may vary depending upon circumstances, but shall always be subject to NATO Security Policy and its supporting directives;

c) reviewing and approving security-related documentation for CIS;

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 reaccreditation 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) exercising independent security oversight over the implementation and operation of the CIS, by coordinating and/or independently executing security audits, by undertaking periodic security inspections or reviews in accordance with the security accreditation process, as well as by reviewing and approving the associated remediation plans should security deficiencies be identified;

g) where applicable, liaising with CISPIAs, CISPs, CISSO, and CISOAs with respect to security risk assessments, on-going security risk management and the acceptance of residual risks by the CISOA;

h) providing direction to the CISPIA, CISP, CISOA, CISSO and other security management staff in responding to and 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 CISPs and CISOAs with 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 with 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 CIS that fall under the scope of this Directive to any other CIS; and

n) where a CIS is required to use assured products, liaising and coordinating with the CISPIA and the appropriate national, international or NATO Evaluation Authority.

6.3. **Management of Security Risks and Compliance**

6.3.1. **Security Risk Management**

6.3.1.1. Security risk management is a systematic approach to determine which security measures are required to protect information and CIS, based upon an assessment of the asset's value, current and predictable threats, vulnerabilities and impact on the mission objectives. Risk management involves planning, organising, directing and controlling resources to ensure that identified risks remain within acceptable bounds.

6.3.1.2. Any security risk assessment is conducted jointly by representatives of the CISOA, CISPIA, CISP, SAA, and the local security organisation, using a security risk

assessment methodology agreed with the relevant SAA[17]. It includes the assessment of the efficacy of existing, enhanced, or new technical measures, including their supporting processes.

6.3.1.3. 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 may be countered and not all vulnerabilities may 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 CIS, by, for example, maintaining secure configuration baselines to keep up to date with the latest threats, analysing the security impact of system changes, following vulnerability and threat management processes, and regularly reviewing and auditing the efficacy of deployed security measures.

6.3.2. **Vulnerability and Threat Management**

6.3.2.1. Any complex system, which could be a CIS or a component of a CIS, is likely to contain vulnerabilities, which may be discovered and exploited at a later stage. Therefore, an accurate knowledge of current vulnerabilities and threats affecting a CIS, as well as a security-sound process that increases the likelihood of discovering and characterising them, are fundamental prerequisites for any risk management process that aims at achieving and maintaining an acceptable residual security risk over time.

Vulnerability

6.3.2.2. 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.

6.3.2.3. To reduce the likelihood and the impact of a potential exploitation of a vulnerability, entities following a security risk management process shall formalise and enable a vulnerability management process in order to prevent, detect, remediate, and monitor vulnerabilities affecting the CIS and its components throughout their life cycle. In line with paragraph 6.3.2.1, the vulnerability management process shall be bound to the broader security risk management framework, to ensure an effective use of available resources and prioritisation of activities, both at local and enterprise level. In this respect, whenever possible, the management of technical vulnerabilities shall take advantage of automation in order to monitor security advisories, detect security deficiencies, and treat them in accordance with the requirements of the SAA.

Threat

6.3.2.4. A threat may be defined, in general terms, as the potential for the accidental or deliberate compromise of security. With regard to CIS Security, such a compromise involves loss of one or more of the security objectives.

6.3.2.5. CIS are attractive targets for intelligence gathering operations, criminals, hacktivists, and terrorists, especially if security measures are ineffective. They can enable

[17] The risk assessment methodology, as well as the level of involvement of the various stakeholders, depends on when, during the life cycle of a CIS, the risk assessment is executed. For example, the authorities involved in a risk assessment during the development of a CIS can differ from the ones involved when the CIS is already accredited and in operation.

large quantities of NATO Information to be obtained quickly and surreptitiously. Any operation carried out by such threat actors (e.g. 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.

6.3.2.6. The insider also represents a unique threat vector to any organisation because of their privileged position with respect to physical and logical access to CIS and the information within them. In contrast to an outsider, insiders have better situational awareness (e.g. knowledge of weaknesses), more time, and legitimate privileges for access to secure areas, CIS and information, by virtue of their 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.

6.3.2.7. Therefore, in order to deter, prevent, detect, and respond to threat actors targeting CIS handling NATO Information, a set of specific security measures shall be defined and implemented.

6.3.3. **Security Accreditation**

6.3.3.1. For CIS that fall under the scope of this Directive, a security accreditation process, or national equivalent approval process, shall be carried out to confirm the CIS can operate while ensuring:

a) NATO Information is protected in accordance with NATO Security Policy and supporting directives; and

b) an acceptable residual security risk has also been achieved and can be maintained over time.

6.3.3.2. During the process of establishing the security requirements, the extent to which CIS Security measures are to be relied upon for the protection of NATO Information and CIS shall be determined.

6.3.3.3. The security accreditation process shall determine that an adequate level of protection has been achieved, can be, and is being maintained. Central to this process is the identification of a level of residual security risk that the SAA deems acceptable, from a NATO Security Policy compliance perspective[18], followed by the correct implementation of the required security measures. The residual security risks shall be then actively monitored and managed by the CISOA and CISP throughout the CIS life cycle.

6.3.3.4. The security accreditation process shall be carried out for CIS that fall under the scope of this Directive, in accordance with the requirements of the Management Directive on CIS Security, and its subsequent revisions.

6.3.3.5. The responsibility for the implementation of the security measures necessary to protect CIS that fall under the scope of this Directive, as well as managing residual security risks, rests with the CISOA. The responsibility for the security accreditation process or national equivalent approval process is assigned to the:

a) relevant NATO SAA for NATO CIS;

[18] For NATO CIS such determination shall be on the basis of a security risk assessment.

b) relevant national SAA, or delegated authority, for national CIS handling NATO Classified Information;

c) competent national authority for other CIS collocated in NATO Civil and Military bodies; and

d) Head of each CoE/ MoU body for their CIS handling non-classified NATO Information or a competent national authority, as appropriate.

6.3.3.6. The SAA retains authority to independently verify that these CIS are built and maintained conformant to the relevant NATO policies, directives and supporting documents addressing CIS Security.

6.3.3.7. Where a NATO CIS falls under the responsibility of more than one NATO SAA, the NATO CIS Security Accreditation Board (NSAB) shall assume the role of SAA or, where deemed relevant by the NSAB itself, a joint security accreditation board shall be established or identified.

6.3.3.8. Security-related documentation shall be established and maintained in accordance with the requirements of the relevant CIS Security directives, internal regulations, and of the relevant SAA. Security-related documentation shall be required throughout the CIS life cycle, from the planning stage until the disposal stage and kept up to date accordingly.

6.3.3.9. When alternative security measures are required to address threats and vulnerabilities affecting mission and safety-critical CIS, the SAA may approve them on the basis of a security risk assessment (conducted during the security accreditation processes) that shall take into account these specific operational aspects of the given system.

6.3.4. **Security Audit**

6.3.4.1. Security audits shall be performed to verify that CIS that fall under the scope of this Directive comply with NATO security policies, directives and supporting documents on CIS Security, and operate in accordance with the security baselines defined by the CISP, in coordination with the SAA. Security audits may also be used to support risk assessments and to prevent or investigate security incidents.

6.3.4.2. Security audit methods include security inspections, reviews, interviews, penetration testing, vulnerability scans, compromise assessments, threat hunting activities, and any generic security testing. When automated tools are used, these shall be trusted, properly configured[19] and, for NATO CIS, governed by a comprehensive Security Classification Guide (SCG). This SCG shall be approved by the relevant NATO Security Authority and shall provide clarification on the classification of audit methodologies, capabilities, indicators, and results.

6.3.4.3. 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 and in coordination with the relevant SAA[20].

[19] The configuration of such tools shall be provided as evidence should this be requested by the SAA or relevant security management staff.

[20] Security Accreditation Authorities may directly execute security audits in support of Security Accreditation efforts and incident response and investigative activities and may utilise trusted industry-provided auditors when they deem necessary.

6.4. Security Education and Awareness

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

6.4.2. The CIS Security education and awareness programme shall make users aware of current threats and vulnerabilities relevant to the CIS they use, in order for them to understand the rationale for, and acknowledge their responsibility to securely operate the CIS. Special attention shall be given to targeted attacks, social engineering and insider threat as these exploit the weaknesses of human behaviours.

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

6.4.4. CIS Security education and awareness shall be provided to users and, in NATO bodies, delivered at least once a year[21]. The CISSO shall determine, based on security risks affecting the organisation (e.g. emerging threats, increased number of CIS Security incidents) whether more frequent security training, education, and awareness sessions are required. In addition, periodic and tailored sessions and training shall be foreseen and provided to staff involved in specific CIS Security activities (e.g. management of crypto material, execution of technical security audits, operators in security operation centres), in major CIS-related projects (e.g. CIS and security architects, security engineers), or employed in high-risk profiles (e.g. administrators, VIP users).

6.4.5. Users' attendance shall be recorded together with the acknowledgment of their understanding. These logs shall be retained by security management staff for auditing purposes.

6.5. Incident Management

6.5.1. A CIS Security incident, or a cyber incident, is any suspected or detected anomaly compromising or that has the potential to compromise a CIS, its supporting services, or any information that is handled in these systems.

6.5.2. Competent and trained management staff shall be designated and made available, based on the internal security regulations and applicable types of security incidents, to proactively and promptly address security incidents and any detected or suspected security breach. These events shall be security investigated by personnel independent from those individuals immediately concerned with the incident. Such personnel shall possess proper security, investigative and, where appropriate, counter-intelligence experience (e.g. Security Officer, CISSO, Counter-Intelligence Officer, NATO Security Authority or National Security Authority);

6.5.3. Supporting processes and procedures shall also be developed and tested regularly for their efficacy against the current threat landscape. An incident response plan shall be composed of different phases and include elements such as the identification of the key decision makers, a way of contacting them, the criteria for incident escalation, the full life

[21] NATO Nations are recommended to deliver training with the same frequency as NATO bodies, unless contingent situations exist that may impede it or risk-based considerations are documented to support a longer delivery cycle.

cycle of incident management, and basic legal or regulatory requirements when CIS Security incidents affect a CIS. The incident response plan shall cover the following phases:

a) a readiness phase to exercise, deter and prevent CIS Security incidents;

b) a process for detecting and notifying relevant Security Authorities, the local security organisation (e.g. CISSO) and CISOAs[22];

c) an incident triage and impact assessment activity;

d) incident containment and threat eradication process and considerations;

e) system recovery and service restoration; and

f) identification of lessons learned and required improvements.

6.5.4. Incidents related to CIS Security shall be reported for response, investigative and inspection purposes in accordance with the conditions set in the NATO Security Policy and its supporting directives, and as requested by the relevant SAA.

6.5.5. Identification, collection, acquisition and preservation of potential digital evidence shall be undertaken by personnel trained in forensic procedures, in a systematic and impartial manner for preserving its integrity, authenticity and admissibility throughout the entire chain of custody and in accordance with relevant legal and policy requirements.

6.5.6. Any relevant information gathered or produced during a CIS Security incident response effort (e.g. Indicators of Compromise (IoCs), discovered vulnerabilities, investigative reports), shall be securely handled and, where required, classified.

6.6. Disaster Recovery and Business Continuity

6.6.1. Disaster Recovery and Business Continuity are key processes that identify potential impacts threatening an organisation's mission should the supporting CIS become unavailable or unreliable. They also provide a framework for building resilience for an effective response that minimises disruption to the organisation and its mission objectives in the event of an incident or crisis.

6.6.2. In this context, 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 relevant DRP and BCP. Both plans shall be maintained and updated regularly by each 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.

[22] In the event relevant authorities (e.g. CISSO, Security Officer, SAA, CISOA) are not available onsite, secure communications means and procedures shall be developed to ensure a prompt notification to the relevant authorities and response to the security incident.

6.6.3. DRPs and BCPs shall be exercised and tested, in NATO bodies, at least every two years[23] to ensure their efficacy and alignment with the requested Recovery Time Objectives[24] (RTOs) and Recovery Point Objectives[25] (RPOs). Records of these exercises shall be retained by security management staff for auditing purposes.

6.7. Third-Party Service Delivery

6.7.1. The term third-party service delivery includes the provision of CIS-related services by industry during the development and/or operations of a NATO CIS or other CIS handling NATO Classified Information.

6.7.2. The NATO Security Policy requires that NATO Classified Information released or created during all phases of the contracting processes, including licensing, bidding, negotiation, award, performance and termination, shall be protected in line with Enclosure "G" titled "Classified Project and Industrial Security".

6.7.3. Furthermore, for CIS that fall under the scope of this Directive, when CIS-related services are outsourced, the CISPIA/CISP and the CISOA, in coordination with the relevant security organisation and the SAA, shall ensure that the requirements for implementation, management, and monitoring of CIS Security measures are formally agreed via SLAs, contracts, or similar legal means that regulate the shared responsibility, to ensure their compliance with the NATO Security Policy.

---

23 NATO Nations are recommended to test Business Continuity and Disaster Recover Plans with the same frequency as NATO does, unless contingent situations exist that may impede it or risk-based considerations are documented to support a longer testing cycle.

24 A targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business and mission continuity.

25 A maximum acceptable period in which data (transactions) might be lost from CIS due to a service disruption.

7. Security by Design

7.1. Definition of Security by Design

7.1.1. Security by Design is a critical CIS Security concept. Security by Design ensures that security is included in the life cycle of all work-related requirements[26], from requirements gathering, solution design and acquisition, through implementation, operation and modification, until its closure or disposal. It aims to enable security based on a number of core principles, including: customer focus, risk assessment and management, creativity, and compliance.

7.2. Secure Design of CIS

7.2.1. Security is dynamic in nature and shall be considered throughout the CIS life cycle. Security requirements and effects shall be reviewed at each stage of the CIS life cycle, from inception to disposal, through an iterative approach that allows the definition of tailored security requirements that can be of organisational, procedural, physical, and technical nature.

7.2.2. Security is an enabler of an organisation's requirements for secure, reliable information sharing and, ultimately, for information superiority, 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. For these reasons, to ensure its effectiveness, security planning shall involve the close interaction between the CISOA, CISPIA, CISP, the relevant security organisation, and the appropriate SAAs.

7.2.3. In order to counter threats and reduce or eliminate vulnerabilities, security shall be addressed at project inception, based on the Security principles (introduced in section 7.4) and starting from the conception of the CIS, so that cost-effective measures can be provided to minimize the security risks anticipated during the design, implementation and operation phases of the CIS life cycle. Measures 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 do the required security measures. CIS planners therefore shall ensure, in coordination with the relevant resource communities, 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.

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

[26] Requirements can refer to any process, product, service, equipment or material purchase, etc.

7.3. **Security Modes of Operation**

7.3.1. Security models and security architectures shall be used to specify how the NATO Security Policy and its supporting directives are enforced in NATO CIS and how the security objectives are achieved.

7.3.2. For CIS handling NATO Information, the indication of the security mode of operation shall be used to describe the security conditions under which the system operates.

7.3.3. CIS handling information classified NATO CONFIDENTIAL and above, or Special Category Information, shall operate in one, or where warranted by mission requirements 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 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 level or at individual's discretion;

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 for the information handled within the CIS; a formal authorisation[27] is required to access any 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 information handled within the CIS.

7.3.4. In the case of multi-level CIS that have users not possessing a Personnel Security Clearance (PSC), the handling of information classified COSMIC TOP SECRET or Special Category information shall not be permitted.

7.3.5. CIS handling NATO RESTRICTED information and NATO CIS handling non-classified NATO Information, shall operate in one, or where warranted by mission requirements 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 have a common need-to-know for all of the information handled within the CIS;

b) "system high" – a mode of operation in which 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 level or at individual's discretion;

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

c) "compartmented" – a mode of operation in which not all individuals with access to the CIS have a common need-to-know for the information handled within the CIS; a formal authorisation is required to access any information handled within the CIS;

d) "multi-level" – a mode of operation in which not all individuals with access to the CIS have a common need-to-know and are authorised to access the NATO RESTRICTED information handled within the CIS.

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

7.4. Security Principles

7.4.1. In order to meet the security objectives, introduced in Section 5, the following security principles shall be used to identify the required security measures to protect a CIS. These security principles shall be followed during the entire life cycle of a CIS, from its initial design until its full decommissioning, in order to ensure that an acceptable security posture can be achieved and also maintained over time.

7.4.2. Additionally, when a Zero Trust strategy is implemented, all principles listed below, as well as those stemming from the relevant DPC Directives, shall be duly considered for the identification of the required security-related measures, processes, technologies, and skillsets in a more granular, dynamic and risk-based Data Centric vision.

7.4.3. Security Principles:

a) Security Risk Management – for NATO CIS[28], formalised security risk management processes shall be applied throughout the life cycle of each CIS to identify, assess, monitor, and treat security risks with adequate security measures and supporting processes. The basis for a sound security risk management approach shall be the identification of an accountable security risk owner, or more than one when required, together with the formal acceptance of any residual security risk, in line with the NATO CIS Security Framework;

b) Secure architecture – security measures shall be designed and implemented using an architectural approach so that they can protect all components[29] of a CIS, its layers[30], its supporting services[31], and ultimately its handled data;

c) Minimality – only the functions, protocols, resources, and services required to carry out the operational mission shall be installed, enabled, and used;

28 The application of a formalised security risk management process within NATO Nations is optional, although encouraged.

29 This term includes Hypervisors, Operating Systems, network devices, databases, applications, containers, security enforcing products, and any other component of the CIS that is running on/off premise, in a cloud environment, on end-users' workstations and on mobile devices and can handle, or may impact the handling of, NATO information.

30 This term includes the front-end, application and backend layers of a generic CIS architecture.

31 This term also includes management and orchestrating services operated by CIS administrators.

d) Least Privilege – all services and users part of, or accessing, any CIS component shall be given privileges and authorisations limited to their duties, their specific tasks, for the least required amount of time, logged and audited by the system;

e) Defence-in-Depth – security measures shall be designed and implemented to ensure multiple lines of defence are in place to protect the CIS, its information, and associated services;

f) Self-protecting element – each CIS, including identified subsystems[32], shall treat each other as untrusted and implement security measures, processes, and procedures, to control the exchange of information among them;

g) Proactive monitoring and detection – monitoring and detecting security measures shall be designed with the assumption that any control meant to prevent security incidents can potentially fail over time and that people make mistakes. As a result, monitoring and detecting measures shall be identified, implemented, and operated accordingly to promptly identify and send alerts on security anomalies and abnormal behaviours within the CIS. These measures shall also enable and support the proactive identification of ongoing malicious activities, including their analysis, containment, delay, and diversion, based on known adversarial tactics, techniques, and procedures (TTPs);

h) 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;

i) Up-to-date Security Posture – security measures shall be designed and operated to ensure they can evolve and scale together with the CIS and they maintain the required level of security while addressing changes in the CIS threat environment;

j) Security Functionality Assurance – the security functionality of mechanisms and products enabling or providing security services to CIS shall be assured by a qualified and trusted authority and shall be implemented in CIS to ensure they fail secure[33]; and

k) Security Compliance –The application of all these principles shall be initially verified, continuously monitored, and regularly assessed by the CISSO under the security oversight of the SAA.

7.5. CIS Security Measures

For NATO CIS, based on the results of a Security Risk Assessment and in line with the NATO CIS Security Principles herein described, all the following technical security measures shall be duly considered for implementation and operation to deter, prevent, detect, withstand and recover from a CIS Security incident.

---

32 In a complex CIS, subsystems can comprise hardware, software, and various supporting processes that fulfil specific mission and business requirements in a defined operational environment. Their identification is done during the design of a CIS and validated as part of the Security Accreditation Process under oversight of the SAA.

33 Unless required not to do so by the SAA, whereby its failure should be risk managed, for example to ensure availability.

7.5.1. **Minimum Security Requirements**

7.5.1.1. For CIS handling NATO Information, there are minimum security requirements to be implemented in order to achieve the required security objectives. These minimum security requirements are set out in Enclosure “F” of the NATO Security Policy, this Directive and the directives and supporting documents on the management, technical and implementation aspects of CIS Security issued by the SC and the DPC.

7.5.1.2. For CIS that fall under the scope of this Directive, when not in contradiction with higher policies and directives, deviations from the minimum security requirements, defined by the SC and the DPC in their directives related to the management, technical and implementation aspects of CIS Security, shall only be authorised by SAAs. 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 appropriate by the SAA for security accreditation purposes; and

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.

7.5.2. **Identity and Access Management**

7.5.2.1. Identity and Access Management is a first line of defence as it provides the identification, authentication, authorisation and accountability of any entity (e.g. person, device, service) requesting access to, and accessing, a CIS, its elements and any NATO Information handled by the system.

7.5.2.2. On CIS that fall under the scope of this Directive, access control measures shall be documented, formalised, and implemented in line with the CIS Security principles, as well as regularly reviewed and audited.

7.5.2.3. Specifically, in the context of access control, Identity and Access Management (IAM) plays a fundamental role as it comprises 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.

7.5.2.4. As a result, access control measures shall be designed and operated to:

a) manage digital identities and their attributes, privileges, and credentials throughout their entire life cycle;

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

c) provide granular authorisation based on access policies;

d) ensure all access to information, by users, services or generic components of a CIS, can be adequately accounted for;

e) restrict and monitor the usage of privileged accounts;

f) audit users and systems activities;

g) prevent credentials and access tokens from being stolen or reused;

h) prevent unauthorised operations on the CIS and related elements (e.g. data, devices, services); and

i) support incident investigations and security audits.

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

a) which and how many different communities of interest[34] will access the CIS, including the specifics of their devices and physical location;

b) technical measures which 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 which 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; and

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

7.5.2.6. Traditional network boundaries are a major element for the security design of a CIS infrastructure. However, the 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.

7.5.2.7. Particularly in such scenarios, the CISPIA shall adopt defence-in-depth strategies which include security policies and measures specific for the protection of information objects[35] 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.

7.5.2.8. Where access by non-NATO nationals to CIS is authorised, measures shall be applied to restrict access only to the NATO Classified Information essential to the non-NATO national's role in achieving NATO's mission. The appropriate SAA, or delegated authority, 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 the CIS.

34 As validated during the Security Accreditation process of the CIS in subject.

35 The wording "information object" may refer to electronic documents, images, videos, audio, database entries, binary or formatted messages, and any other type of electronic data that contains or represent NATO information.

7.5.2.9. Minimum requirements for identification and authentication on CIS that fall under the scope of this Directive are set out in the Technical and Implementation Directives on CIS Security issued by the DPC 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.

7.5.3. **Application Security**

7.5.3.1. Authentication and authorisation controls to grant access to information are commonly enforced at the application level. As a result, the compromise of an application, or its supporting services[36], can often allow adversaries to access any information processed by them.

7.5.3.2. To counter these scenarios, security shall be embedded in the life cycle (design, development, deployment, maintenance) of software applications and services purposely developed, implemented, or customised to handle NATO Information[37]. The required security measures shall be determined following the NATO Security Principles and shall be aligned with the CIS Security Objectives.

7.5.3.3. General-purpose software applications shall also be subject to security testing, and their operations compliant with the CIS Security Management System and CIS Security Operations requirements set in this document.

7.5.3.4. Similarly to CIS, the principle of "self-protection'' shall be applied for software applications and services. These shall be protected by security measures preventing and detecting attempts to compromise their security by end-users or from other interconnected applications.

7.5.4. **Malware Defence**

7.5.4.1. 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.

7.5.4.2. On CIS that fall under the scope of this Directive, malicious code detection solutions shall be utilised to block installation, prevent execution, quarantine malicious software and alert personnel responsible for incident response activities.

7.5.5. **Endpoint Protection**

7.5.5.1. The weakest link in the chain of CIS Security is often the human element. To protect a CIS it is therefore fundamental to protect and secure users' endpoints (e.g. official workstations, terminals, and mobile devices) with the assumption that users, either willingly or accidentally, will often pose a threat to the system.

---

[36] Supporting services in this context does not refer to infrastructural services, but rather software services that are provided to an application as part of a cloud, virtualised or micro-services architecture.

[37] For NATO CIS, the design, implementation and operations of these applications shall be compliant with the NATO CIS Security Framework, including Security-by-Design and Security Operations requirements.

7.5.5.2. To this end, security measures shall be implemented and maintained to ensure end-users accessing services on less trusted CIS (such as internet-based services) are protected against external threats aiming at compromising the user's CIS, including their credentials and endpoints.

7.5.5.3. In addition, endpoints shall keep an acceptable security posture over time to minimise risk to NATO Information. Overall, they shall be compliant with NATO Security principles and operated accordingly with this Directive.

7.5.5.4. The implementation of security mechanisms to detect and prevent leakage of information from the CIS (including through users' endpoints) shall be duly considered, commensurate with the impact on the security objectives of the CIS.

7.5.5.5. Due to ever evolving techniques used by adversaries to bypass antimalware products, the organisation shall employ formal procedures and enforce technical measures to limit users from installing and executing non-authorised software. Users' endpoints shall also employ security measures to protect against the so called "file-less malware" attacks where legit services from the operating system are abused to run malicious instructions directly in the memory. All these protecting measures shall be complemented by security logs and detecting mechanisms to monitor and audit those events that may reveal a compromise of the users' endpoints.

7.5.5.6. On CIS that fall under the scope of this Directive, CISPs shall maximise the use of automated tools to only allow the use and execution of authorised applications and scripts.

7.5.6. **Security-Related Logs**

7.5.6.1. CIS that fall under the scope of this Directive shall be protected by security measures for the detection of malicious activities and faults, through the secure collection, review and storage of information for security-related events.

7.5.6.2. 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.

7.5.6.3. 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 CISSOs and SAAs.

7.5.6.4. Security logs shall be protected, reviewed, and retained as defined by the relevant CISSOs in coordination with the SAA.

7.5.6.5. A detailed list of security log requirements shall be based on the results of a risk management approach which considers any other factor deemed relevant by the authority responsible for the security accreditation, and includes the following:

a) security objectives of the CIS;

b) threat environment;

c) type of logs and data collected;

d) frequency of log reviews;

e) log authenticity requirements[38];

f) use of automated tools in support of log analysis and review;

g) investigative, audit and legal requirements; and

h) compliance with applicable NATO Security directives.

7.5.7. **Cryptographic Security**

7.5.7.1. The requirements relevant to cryptographic security are set out in Enclosure "F" of NATO Security Policy and in the related Technical and Implementation Directives issued by the DPC.

7.5.8. **Emission Security**

7.5.8.1. The requirements relevant to emission security are set out in Enclosure "F" of the NATO Security Policy and in the related Technical and Implementation Directives issued by the DPC.

7.5.9. **Trustworthiness Management**

7.5.9.1. Trustworthiness in CIS Security is a complex issue that involves 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).

7.5.9.2. Security functionalities of CIS that fall under the scope of this Directive and related products shall be assured by trusted and qualified authorities through formal assurance techniques.

7.5.9.3. Formal assurance techniques for products include:

a) Evaluation – the independent analysis, by the appropriate national, international or NATO evaluation authority[39], of the security aspects of a product[40]. The evaluation confirms the presence, correct functioning and incorruptibility of security functionality consistent with the requirements and/or principles published or accepted by a national evaluation authority. The evaluation determines the extent to which the security claims for a product are satisfied and establishes the

[38] Depending on the operational context of the CIS, security logs left on a compromised system are not deemed reliable to support a security investigation.

[39] The national evaluation authority may delegate the evaluation work to an entity that the national evaluation authority has formally qualified to perform evaluation work under a national or international evaluation scheme.

[40] Any analysis supporting the evaluation of Security Enforcing Products shall account for relevant NATO Security Technical and Implementation Directives issued by the DPC. Furthermore, the evaluation may also include an analysis of the relevant development and operational processes that are followed by the provider of the product.

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;

b) Certification – 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 – 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.

7.5.9.4. For CIS that fall under the scope of this Directive, security enforcing products in the categories of cryptographic equipment[41], 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 a National CIS Security Authority (NCSA), or other competent national authority.

7.5.9.5. Formal assurance techniques for CIS include:

a) Security evaluation – the independent examination, by the appropriate national or NATO authority, of the security aspects of a CIS. The security evaluation determines whether the CIS satisfies its pre-defined security requirements and can be supported by different types of security audits;

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

7.5.9.6. Overall, assurance requirements for CIS that fall under the scope of this Directive shall be identified in the CIS planning phase by the CISPIA, in conjunction with the SAA. This shall take into account the requirements set in the Enclosure “F” of the NATO Security Policy and supporting Directives, and, whenever applicable, an assessment of the security architecture and the outcome of the security risk management process.

7.5.9.7. Assurance requirements for cryptographic products or mechanisms shall be in accordance with the provisions of Enclosure “F” of the NATO Security Policy and relevant Technical and Implementation Directives and supporting documents on CIS Security.

7.5.9.8. When evaluation and certification of products are required, the Common Criteria methodology (or national or international equivalent) shall, where appropriate[42], be used[43].

---

41 As required by Enclosure F of the NATO Security Policy, cryptographic products used to protect the confidentiality of information classified NS and above shall be approved by the Military Committee. Specific security requirements, including associated approval processes, shall be sought in Enclosure F and in relevant NATO Security Technical and Implementation Directives.

42 Not applicable to cryptographic and TEMPEST products.

43 When the Common Criteria methodology is used, the CISPIA or CISP shall provide to the SAA, upon request, relevant product certification artefacts such as the Target of Evaluation, Protection Profile, and Security Target.

7.5.9.9. The use of security-enforcing hardware, firmware and software[44], 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.

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

7.5.9.11. 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 with the requirements set out in Enclosures "F" and "G" of the NATO Security Policy and supporting directives.

7.5.10. **Interconnection of CIS**

7.5.10.1. Very often, in order to fulfil their mission and share information, 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 the "self-protecting element", it is necessary to address the potential risks posed by interconnecting, directly or through a cascading interconnection, a CIS handling NATO Information to another CIS by implementing specific and tailored security measures.

7.5.10.2. In the context of CIS Security, an interconnection is defined as the capability that enables the intended bi- or unidirectional flow of information between two CIS over an established connection. When instead a CIS is using another system purely as a transport layer (e.g. a geographically dispersed CIS relying on governmental networking links to transport services to various locations) this is not considered as an interconnection, but the security posture of the bearer system shall be accounted as part of the accreditation efforts of the overlaying CIS and its interconnections[45], and vice versa.

7.5.10.3. For all interconnections of CIS that fall under the scope of this Directive, the following shall be subject to the approval of the relevant SAA(s)[46]:

a) the method of interconnection[47], the services provided through the interconnection as well as any new additional type of data and information flow and, where applicable, new users' communities, their equipment and physical locations;

b) for NATO CIS, the methodology, scope, and results of security risk assessment and risk management processes;

---

44 Procurement requirements for cryptographic products or mechanisms are specifically defined in relevant Technical and Implementation directives developed by the DPC.

45 For NATO CIS through a formal security risk assessment that identifies those risks that are inherited from the underlying infrastructure and can affect the security objectives of the overlying CIS.

46 In scenarios where the interconnection is among two CISs that fall under the responsibility of two different SAAs, both of them shall approve the request for their interconnection.

47 For NATO CIS the design, implementation and operations of any interconnection shall be compliant with the NATO CIS Security Framework, including its Security-by-Design and Security Operations requirements.

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

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

7.5.10.4. While the supporting Management Directive on CIS Security and its subsequent revisions also sets out specific security accreditation requirements for interconnections, the supporting Technical and Implementation Directives on CIS Security further define the specific measures to be implemented.

7.5.10.5. The requirement for protective measures for CIS handling NATO Information which are interconnected to the Internet or similar networks in the public domain arises from the exceptional security risks posed by these types of public networks. CIS handling NATO Classified Information are at unacceptable security risk when interconnected to Internet or similar networks in the public domain, unless specifically protected as prescribed by the NATO Security Policy and its supporting directives.

7.5.10.6. The direct or cascaded interconnection to Internet or similar networks in the public domain of CIS that fall under the scope of this Directive up to and including NATO SECRET shall be:

a) strictly controlled;

b) subject to the validation of the security requirements by the SAA;

c) subject to evaluation and certification and/or approval of the security enforcing mechanisms as identified in 7.5.10 and supported by relevant Technical and Implementation Directives on CIS Security issued by the DPC and by the SAA;

d) for NATO CIS, subject to formal vulnerability, threat and security risk management processes; and

e) subject to periodic security audit[48] from a competent authority[49].

7.5.10.7. The direct 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. Cascaded interconnections may be approved by the SAAs, following a formal request by the relevant CISOAs, subject to the satisfactory compliance of the end-to-end information flow[50] with all security conditions set in the previous paragraph.

NATO Information on Internet or similar networks in the public domain

7.5.10.8. CIS handling NATO Classified Information may use the Internet or similar networks in the public domain purely as a bearer, provided that the appropriate

48 At a minimum a Type 3 Security Audit (T3SA) is required on a periodic and risk-informed basis as defined in AC/35-2005-REV3, Management Directive on CIS Security, and subsequent revisions.

49 The appointment of the competent authority in charge of conducting security audits shall be concurred with the relevant SAA.

50 In a cascaded interconnection the end-to-end information flow requires the concatenation of two or more interconnections and its security shall be assured by at least three different and sequential CIS.

cryptographic protection is implemented. In this instance, all security objectives shall be seriously considered.

7.5.10.9. CIS may use a public cloud environment for handling NATO RESTRICTED information, if the CIS and the Cloud Service Provider are compliant with the security requirements stemming from this Directive and any other applicable CIS Security Technical and Implementation Directive on the protection of NATO RESTRICTED information in a public cloud environment.

7.5.10.10. 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) NATO UNCLASSIFIED information that, as determined by the originator(s), bears no additional administrative marking (e.g. medical) or dissemination limitation marking to indicate the sensitivity of the information[51].

7.5.10.11. 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.

7.5.11. **Security Management Infrastructure**

7.5.11.1. Enclosure “F” of the NATO Security Policy 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)[52] shall be established to ensure that the capabilities managing CIS Security-related services, processes and devices across NATO bodies are managed securely and as an enterprise.

---

51 Some NATO UNCLASSIFIED information may be determined by the SAA as being sensitive and therefore require encryption when transmitted over a public network or therein stored. This could include information relating to security-related mechanisms such as user credentials and access tokens which could be used by an adversary to masquerade as that user.

52 Examples of SMI include multi-tier administrative architectures, (sub) networks within a CIS dedicated to management activities, etc.

8. CIS Security Operations

Security Operations covers security requirements for CIS that fall under the scope of this Directive that shall be followed during the operations of a CIS up to its decommissioning. Based on a shared responsibility model, if any, the CISOAs are responsible for the correct implementation of the following security requirements, as identified in this section.

8.1. Asset and Configuration Management

8.1.1. A prerequisite to run an effective risk management process, and to efficiently execute any security-related activity, is the ability to determine at any time during the life cycle of a CIS which hardware and software components are part of it, what is their role in its architecture, and which supporting services are provided by external entities to ensure its correct functioning.

8.1.2. The CISP, in close coordination with the CISOA, CISSO, and CISPIA, shall maintain a list of all CIS assets, that shall include, at a minimum, information on their configuration, a description of the provided functionality, their business and risk owners. Such activity shall be supported by documented and formalised procedures developed by the CISP and endorsed by the relevant CISOA and CISSO, in coordination with the SAA.

8.1.3. Among the identified assets, and as part of the security risk assessment, special attention shall be given to those assets in the CIS deemed “critical”. These critical assets are defined as those CIS components whose failure in terms of integrity or availability also plays an important role and can lead to a detrimental, up to an exceptionally grave, damage to NATO missions and objectives. Critical assets may include, depending on the operational context of the CIS and as endorsed by the relevant SAA:

- Routing devices;
- Name resolution services;
- Hardware Security Modules (HSMs) and software Key Vaults;
- Electronic Security devices supporting physical security measures;
- Building Management Solutions;
- Command and Control (C2) communication elements[53];
- Global Positioning Systems or equivalent; and
- Any other type of equipment which may directly cause, should its integrity be compromised, a denial of service to the CIS or associated services.

8.1.4. On CIS that fall under the scope of this Directive, security baselines for CIS, its components, and their supporting services shall also be defined, enforced and kept up to date through configuration management and change control processes during the entire CIS life cycle.

[53] This category can include CIS components supporting satellite, terrestrial, and maritime communications.

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

8.1.6. The CISP shall regularly review current configuration baselines to ensure they continue to be effective against the current threat landscape and known vulnerabilities. This review shall be aligned with the Vulnerability and Threat management processes of the organisation and the SAA shall be notified of their update.

8.2. **Change Management**

8.2.1. During the life cycle of a CIS, hardware and software changes can usually be introduced following new and enhanced business requirements[54], new vulnerabilities and threats being discovered, or in response to a security incident. However, because any change can potentially impact the security posture of the CIS, a formalised and structured change management process shall be defined and implemented.

8.2.2. The change management process shall be formalised and shall address, at a minimum, the following aspects:

a) a description of the required change and the reason for being implemented;

b) an accountability for all actors involved in the request, approval, and implementation of the change;

c) an assessment of potential security impact to the CIS and its users. This analysis shall also assess the implication of the change to the current Security Accreditation Status and the requirement to involve the SAA; and

d) a specification of how the change will be tested, evaluated and eventually implemented in the required environment (e.g. test, reference, and production environments); and

e) a roll back procedure, when necessary.

8.3. **Patch Management**

8.3.1. Hardware and software vulnerabilities are continuously discovered and publicly disclosed, making the CIS and its components always susceptible to new attacks. In response, a patch management process shall be formalised and implemented to ensure the security posture of the CIS is maintained effective over time.

8.3.2. The patch management process shall cover not only Operating Systems, but also applications, libraries, firmware and appliances. Whenever possible, and as coordinated with the CISSO and SAA, the CISP and CISOA shall agree on using automated systems to deploy, test and validate security patches.

8.3.3. For CIS that fall under the scope of this Directive, the patch management process shall identify implementation timelines in line with the risk faced by the CIS and the severity of the vulnerabilities. The process shall also be aligned with existing Change and

[54] In this context, new business requirements include both functional and non-functional specifications.

Configuration Management processes, as well as Vulnerability Management practices employed by the organisation.

8.4. Handling and Control of Removable Computer Storage Media

8.4.1. The security classification level of all removable computer storage media[55] holding NATO Classified Information shall be easily identifiable (such as by bearing 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 shall indicate the highest classification of information that shall ever be stored on the individual media item. The security classification can only be reduced if downgraded according to approved procedures.

8.4.2. 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, physical security, and industrial security directives. 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 regularly spot checked for their physical presence and contents (to ensure that an inappropriate Special Category is not stored on the media); and

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

8.4.3. Additional controls may be mandated by the SAA and CISOA for media holding information bearing other security classification markings.

8.5. Backup Management

8.5.1. A backup management process shall be identified and implemented to support the organisation's Business Continuity and Disaster Recovery plans.

8.5.2. Information stored in backups retain the same classification unless securely and properly encrypted in compliance with NATO Security Policy and supporting directives. As a consequence, backups carry all security requirements already applicable to the information handled by the CIS, including those applicable to Removable Computer Storage Media.

8.5.3. In addition, backup management procedures and processes shall be formalised within the organisation, in line with additional requirements stemming from the NATO

[55] A removable computer storage media is a type of storage media that can be inserted and removed from a CIS (e.g. USB pen drives, CD ROM/DVD, hard drives), shall be considered equivalent to documents, and protected with a level equivalent to that applicable to hardcopies at the same classification level.

Security Policy in the domains of physical security, security of information and industrial security.

8.5.4. Backup management procedures and processes shall allow the determination, at any moment, of the following:

a) where the data backups are located;

b) which physical security measures are applied for their protection;

c) how access to the media is controlled;

d) how backups are reused and/or disposed; and

e) when the backups were last tested and whether the test could meet the established Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

8.6. Decommissioning of CIS and Equipment

8.6.1. During the life cycle of a CIS, in order to ensure the organisation continues to meet its business and operational requirements, it is common practice that some of the CIS components are replaced or the whole CIS decommissioned at the end of its life.

8.6.2. Therefore, to ensure NATO Information is protected during such critical activities, the CISOA shall ensure that the required security measures, processes, and contractual agreements, where relevant, are not retroactively implemented and enforced, rather they are in place before the system or its components cease to operate.

8.6.3. As a result, depending on the operational context of the CIS, at a minimum, the following security requirements shall be considered at the earliest stages of a CIS life cycle:

a) a secure downgrading, declassification, and destruction plan of all electronic CIS equipment and Storage Media, in accordance with this Directive and the related Technical and Implementation Directives issued by the DPC;

b) a data migration plan from the legacy CIS to a new system, should the former be replaced;

c) a termination or migration plan for all relevant interconnections that are used by the system under decommissioning; and

d) a retention plan of the following CIS-related information:

- all the relevant documentation that was created and approved during the security accreditation process;
- any security audit report, associated findings, and remediation plan; and
- security logs generated by the CIS.

The retention period for the above-mentioned information shall be determined based on the classification level of the CIS and in accordance with latest revision of the Directive on the Security of NATO Classified Information (ref. AC/35-D/2002) and relevant Technical and Implementation Directives.

8.7. Downgrading, Declassification and Destruction of Computer Storage Media

8.7.1. NATO Classified Information electromagnetically or otherwise recorded on reusable computer storage media, shall only be downgraded in accordance with the NATO

Security Policy, its supporting directives, and procedures approved and stated in the security-related documentation.

8.7.2. When a computer storage medium comes to the end of its useful life, it should be declassified whereupon it may be released and handled as unclassified. If the medium cannot be declassified, or poses an unacceptable risk to the integrity and/or availability of the information due to a potential failure of the medium, it shall be destroyed following an approved security procedure. Computer storage media which have held NATO SECRET, COSMIC TOP SECRET or Special Category information, for example ATOMAL and US-OPLAN, may be destroyed but shall not be declassified.

8.8. **Use of Privately-Owned Equipment for Official NATO Work**

8.8.1. The use of privately-owned equipment, including removable computer storage media, software and hardware (e.g. PCs and portable computing devices) shall be prohibited for storing, processing and transmitting NATO Classified Information.

8.8.2. Privately-owned hardware, software and media shall only be brought into a Class II security area, where NATO Classified Information is stored, processed or transmitted, after a security authorisation is provided in accordance with the appropriate NATO/national, Strategic Command or Agency regulations.

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

8.9.1. 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.

Appendix 1 – Additional Requirements Applicable to NATO Bodies and NATO CIS

1. Roles and responsibilities

CIS Security Officer (CISSO)

1.1. The following and additional security oversight responsibilities are assigned to a NATO CISSO:

a) oversee the management of CIS Security risks and reporting them annually to the relevant Security Accreditation Authority (SAA), together with the Security Accreditation Status of all NATO CIS in use by the body;

b) support the security organisation in the development and execution of the internal security regulations, which shall be coordinated with, and endorsed by, the relevant NATO Security Authority before being implemented and used by the organisation; and

c) for NATO CIS, if an insider threat is suspected, the CISSO shall immediately notify the NOS, preferably through secure channels, seeking direction and guidance on any incident response and investigative activity that shall be conducted on the system and inside their organisation.

NATO Enterprise CISOA and Single Point of Authority (SPA) for Cyber Security

1.2. At NATO, the OCIO is the Enterprise CISOA and SPA for Cyber Security for all NATO bodies falling under the scope of “The NATO Enterprise” and the “NATO Owned and Operated Networks”, both concepts defined by the DPC.

1.3. In this context, the OCIO shall assume the role of CISOA for all NATO Enterprise CIS, namely when a NATO CIS supports simultaneously core-business requirements of more than one NATO CISOA and is not limited to individual communities of interest. Furthermore, in view of its role of Single Point of Authority for Cyber Security, it shall be responsible for:

a) defining, implementing, and overseeing the execution of an overarching risk management framework for the NATO Enterprise, in compliance with the NATO Security Policy, that accounts for a federated model, individual mission and business requirements, and with the objective of enabling an effective and coherent risk-informed decision-making process across the whole enterprise;

b) setting the NATO Enterprise strategic direction, issuing guidance, and working with individual NATO Enterprise entities (e.g. other CISOAs), to ensure Cyber Security activities stemming from this Directive, as well as those supporting the NATO Enterprise risk appetite, are coherently and consistently performed across the enterprise;

c) ensuring Cyber Security requirements are included at the earliest phases of the capability development process for NATO Enterprise solutions;

d) ensuring that the relevant SLAs or similar mechanisms, established with the CISPs for the provision of Enterprise solutions, include the requirements for an effective

implementation, operation, monitoring, and change management of security measures;

e) providing direction to the NCI Agency, NATO Cyber Security Centre (NCSC), to ensure Cyber Security services provided by the Agency to the NATO Enterprise are consistently and effectively operated;

f) acting as top-level cyber incident manager for the NATO Enterprise and ensure cyber incidents affecting the enterprise can be prevented, detected, and responded upon; and

g) defining and monitoring the execution of a NATO Enterprise Vulnerability Assessments Plan (EVAP) in a coordinated and prioritised manner, harmonizing technical, security and operational requirements enterprise-wide. This plan shall include the security review of the NATO external cyber attack surface, internal vulnerability assessments (e.g. Online Vulnerability Assessments (OVAs) and T3SA), Penetration Testing (i.e. T4SA), Adversary emulation activities, and EMSEC-related testing[56]). In this respect, the planning and execution of the EVAP shall be coordinated by the OCIO with the relevant stakeholders, annually approved by the BCISOA and endorsed by the NSAB.

1.4. In addition, when a NATO CIS is provided at the level of the NATO Enterprise, or when multiple interconnections exist amongst NATO bodies, all relevant CISOAs shall coordinate through the NATO Board of CISOAs (BCISOA), chaired by the OCIO, to ensure a harmonious approach to security risk management in line with the NATO Security Policy.

1.5. Similarly, when a NATO CIS is provided to NATO Nations, the execution of the functions mentioned above shall be coordinated also with the National CISOAs (e.g. through a Board with National CISOA representatives) and relevant NATO stakeholders (e.g. OCIO, NHQ Digital Staff, NSAB), to avoid inharmonious approaches between the NATO Enterprise and those elements in the Alliance that rely on NATO CIS.

1.6. Finally, to ensure the required Cyber Security activities are planned and executed in line with the NATO Security Policy and its supporting directives, the OCIO shall closely coordinate and liaise with the NATO Security Authorities who remain responsible for monitoring compliance against the NATO Security Policy and shall be involved in the agreement of the security risks to be accepted.

2. Management of Security Risks

2.1. NATO Security Risk Management

2.1.1. In NATO bodies, the organisation shall formalise and employ a security risk management process, in line with the NATO Security Policy and its supporting directives that shall be applied throughout the life cycle of each and every CIS. The security risk management framework shall be approved by the Head of the organisation, by the security

[56] Security findings affecting CIS or organisations that do not belong to the NATO Enterprise, shall be reported by the auditor only to the relevant NATO/National/NNE Security Authority and to the affected entity.

organisation (e.g. CISSO), coordinated with the OCIO, and be subject to endorsement by the relevant NATO Security Authority (e.g. NATO Office of Security).

2.1.2. Security risk management processes shall be applied to identify, monitor, reduce, transfer, eliminate, avoid or accept risks associated with NATO CIS. The aim is to select a solution which results in a satisfactory trade-off between functional requirements, resources, and residual security risk(s) whilst ensuring that required security measures and processes are applied for the protection of NATO Information, in accordance with the requirements of NATO Security Policy and supporting directives.

2.1.3. For NATO CIS, security risk assessment, as part of security risk management, shall be embedded in the system development life cycle, shall be based on an up-to-date threat analysis, and shall identify the impact of threats and vulnerabilities on the achievement of the security objectives and the organisation's mission.

2.1.4. At least on an annual basis, the residual security risks for all NATO CIS in the organisation shall be qualified, quantified, and formally accepted by the relevant CISOA, in coordination with the OCIO. The residual security risks shall be reported[57] annually, or earlier should the security risk level increase significantly, to the relevant SAA. In the event some NATO CIS are not security accredited, or when residual security risks are not deemed compliant with the NATO Security Policy by the SAA or acceptable by the CISOA, the organisation shall also submit a remediation plan describing all activities that will be executed to reach and maintain compliance with the NATO Security Policy, its supporting directives, and the CIS Security risk appetite of the relevant CISOAs.

2.2. Vulnerability and Threat Management

Vulnerability Management

2.2.1. On NATO CIS, CISPs shall maximize the use of automated tools for vulnerabilities discovery and remediation, in line with NATO-approved baselines and remediation timelines.

Threat Management

2.2.2. In the selection of security measures meant to deter, prevent, detect, and respond to threat actors targeting CIS handling NATO Information, NATO bodies shall take into account the following:

a) a comprehensive threat management programme, accompanied by a programme security classification guide (SCG), shall be followed to determine current and anticipated security threats to the CIS environment. The analysis shall identify tactics, techniques, and procedures (TTPs), used by threat actors relevant to NATO,

[57] When technologies allow, this and other reporting requirements set out in this Directive shall be implemented via automated means (e.g. SAA able to access, in read-only mode, risk management tools used by the CISOA). This is meant to ensure timely reporting while reducing manual work by the CISOA/CISSO, and still ensuring a proper oversight by the SAAs.

with the objective of supporting a comprehensive risk management process in the organisation, including the secure design and operation of the CIS;

b) specific security measures and processes shall be designed to cope with insider threats and support tailored incident response and investigative procedures. Such process shall be supported by a close coordination and information sharing among the internal or external organisational elements (e.g. Personnel Security, Physical Security, Human Resources, Intelligence); and

c) For NATO CIS, investigative procedures for Insider Threats may be supported by technical solutions able to analyse and predict the behaviour of CIS users and administrators (e.g. User Behaviour Analytics - UBA solutions). The relevant NATO SAA, or counter intelligence authority, shall be granted access to these and similar capabilities, as required, and following agreed procedures that do not hinder the effectiveness of a security investigation.

3. Security Audits

3.1. In addition to the requirements set at paragraph 6.3.4 at Annex 1, to ensure an efficient and punctual execution of security audits on NATO CIS, CISOAs shall formulate an annual security audit plan, on a security-risk basis, that shall be coordinated with the OCIO, endorsed by the relevant SAAs, and monitored by the parties during its execution.

3.2. For NATO CIS, security audits shall be also carried out to:

a) assess the effectiveness of CIS Security processes and capabilities by means of measures and measurement;

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

c) verify that the security measures, resultant from the security risk management process, are correctly implemented and maintained throughout the CIS life cycle;

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

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

4. Security Compliance

4.1. In NATO bodies, security management staff shall monitor the application and implementation of the NATO CIS Security Framework, including its security requirements, measures, and processes, across the whole organisation.

4.2. In NATO bodies, the CISSO shall also have full visibility and report to the Head of the organisation and, annually, to the SAA, on all CIS and their current security risk level, including their Security Accreditation Status. Commensurate with evolving risks and where deficiencies are identified, these shall be addressed by the relevant CISOA.

5. Incident Management

5.1. CIS Security incidents affecting NATO CIS shall be reported to the OCIO[58], in its role of top-level incident manager for the NATO Enterprise, to NCI Agency/NCSC and responsible CISSO, in compliance with the Internal Security Instructions (ISIs) or SecOPs of NATO Civil or Military bodies and in accordance with the incident reporting formats and guidelines defined by the NCIA/NCSC and/or security investigative authorities.

5.2. The Directive on the Security of NATO Classified 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 threats, including privileged administrators);

f) incidents involving privileged access to CIS;

g) incidents involving cryptographic elements; and

h) incidents causing a significant impact to the organisation.

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

5.4. For NATO CIS, an SCG shall be approved by the relevant NATO Security Authority and used to determine the relevant security handling requirements.

6. Third-Party Service Delivery

6.1. In addition to the requirements set in section 6.7, for NATO CIS the procurement and contracting processes shall be supported by due diligence activities to ensure third parties, who are providing CIS-related solutions and services to NATO, can protect NATO Information and, where relevant, NATO CIS, in compliance with the NATO Security Policy and its supporting directives. In this respect, NATO bodies shall employ maturity-based criteria during the selection of a third party with the aim of assessing:

a) the provider’s risk, compliance, vulnerability and threat management processes;

b) the level of security assurance of their solutions and their alignment with NATO Security Principles and requirements;

c) how the provider documents, manages, and measures its security-related processes;

[58] Exceptions apply when the CIS Security incident is potentially related to the activities of an insider threat and information carrying special markings.

d) what security measures are implemented by the provider to secure information released by NATO or created in support to the project;

e) the level of competency and skill of the proposed personnel;

f) supply-chain security processes employed by the provider for the secure procurement of CIS products, not limited to Security Enforcing Products, and in line with relevant NATO directives;

g) provider's plan to support changes in the procured products should vulnerabilities be discovered; and

h) provider's plan to respond to an internal incident impacting NATO Information or NATO CIS.

6.2. On a case-by-case basis, and subject to a prior agreement with the relevant SAA, the compliance of a third-party service provider with internationally-recognised standards can be used by NATO contracting authorities as evidence that the previously mentioned criteria are met by the provider. In such circumstances, the third party shall make available to the NATO contracting authority and the relevant SAA, any technical, procedural, or financial artefact that is requested by either authority. This approach shall not be used in place of formal assurance techniques meant to determine the trustworthiness of products or CIS (reference 7.5.9) or to circumvent the security requirements laid down in Enclosure G to C-M(2002)49-REV1 and its supporting directive.

7. Continuous Security Improvement

7.1. For NATO CIS, the implementation of a proper CIS Security Framework shall help the organisation in making security-related activities more effective, efficient, and aligned with mission objectives. To this end, a continuous[59] security improvement process shall be identified in NATO bodies to promptly detect and manage security gaps as well as to consider the organisation maturity[60] from a CIS security perspective.

7.2. In each NATO body this process shall be based, at least, on the annual results of the security risk management process, a threat management programme, the trend of security incidents that affected its CIS, and the outcome of security audits.

7.3. All this input shall result in the definition and update of a formal CIS Security strategy, and associated implementation roadmap, that shall be coordinated with the OCIO and endorsed by the relevant NATO Security Authority.

7.4. In addition, the security reporting to the three NATO Security Authorities, as prescribed in this Directive, shall be used by these Authorities to:

---

[59] The frequency can depend on available resources, threat landscape affecting the CIS, and the overall security posture of the organisation.

[60] In the context of this document and in the Management Directive on CIS Security (including its subsequent revisions) an organisation may be considered mature when the organisational CIS Security processes are documented, executed in a repeatable and coordinated manner, as well as reviewed for effectiveness and efficiency on a regular basis.

a) highlight areas of security concerns that are common to different NATO bodies and which shall be reported to the Board of CISOAs (by their respective CISOA representatives) and addressed during the security accreditation of NATO CIS;

b) ensure a consistent and corporate approach to the security of NATO CIS;

c) plan more effectively for technical Security Audits and security inspections in NATO bodies; and

d) provide inputs to the Security Committee during the revision of the NATO Security Policy and its supporting Directives

8. NOS Security Oversight

8.1.1. Enclosure “B” of the NATO Security Policy defines the role of the NATO Office of Security and its responsibilities with respect to security for NATO. In this context, the NOS is responsible to inform, as appropriate, the SC, the Secretary General (SG) and the Chairman of the Military Committee (CMC) of the security within NATO, and the progress made in implementing NAC decisions in the domain of security.

8.1.2. For NATO CIS, the following events are specifically subject to security oversight and may trigger a security incident procedure, as deemed necessary by the NATO Security Authorities, and may require a notification to the SC, SG, and CMC by the NOS:

a) lack of a formalised security organisation within a NATO body which is approved by the relevant NATO Security Authority;

b) any NATO CIS handling NATO Classified Information without being security accredited[61];

c) any security incident involving NATO CIS which is not followed by a formal incident response and notification to the relevant NATO Security Authority;

d) any non-conformity with NATO Security Policy and its supporting directives which is not addressed in the period between two inspections; and

e) any delay longer than 6 months in providing to the relevant NATO Security Authority the requested annual security deliverables, as defined by the herein introduced CIS Security Framework:

   i. annual results stemming from the execution of the security risk management process;

   ii. annual overview on the accreditation status of all NATO CIS in the organisation;

   iii. annual organigram of the security management staff in the organisation;

   iv. annual results of the continuous improvement programme; and

[61] This scenario can also occur when the security accreditation process has been followed in its entirety by the CISPIA/CISP/CISOA, but it has been determined that the system cannot operate with an acceptable residual security risk.

v. results of the most recent Disaster Recovery and Business Continuity exercise, which shall be no older than three years.

Appendix 2 – NATO CIS Security Policy Governance

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 NATO Security Policy;

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

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

(d) the Cyber Defence Committee (CDC) responsible for the Cyber Defence Policy; and

(e) the Military Committee (MC) for military requirements.

2. Additional NATO and national bodies directly or indirectly involved in CIS Security matters are listed at Appendix III.

Appendix 3 – 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 CIS Security Authorities (NCSA);

(d) National Tempest Authorities (NTA);

(e) National Distribution Authorities (NDA); and

(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 Digital Policy Committee (DCP), and its Capability Panel on Information Assurance and Cyber Defence (CaP4);

iii. the Military Committee (MC) for military requirements; and

iv. the Cyber Defence Committee (CDC) for the NATO's Cyber Defence Policy.

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

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

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

(c) NATO staff support in NATO Headquarters:

i. the NOS, for executing the overall oversight of all security matters at NATO and for providing independent security advices and recommendations in line with NATO Security Policy and its supporting directives;

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

iii. the Office of the Chief Information Officer (OCIO) in its role of Enterprise CISOA, Single Point of Authority on Cyber Security at NATO, NATO Coherence Authority, and as the Chair of the Board of CISOAs; and

iv. International Staff (IS), including the Innovation, Hybrid and Cyber Division (IHC) 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; and

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; and
- 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 (CIS), ICT-related services, and for providing specialist cyber-security services to NATO bodies throughout the lifecycle of NATO CIS;

iv. the NATO School of Oberammergau (NSO) and the NATO Communications and Information Academy (NCI Academy);

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

vi. the Board of CISOAs (BCISOA); and

vii. the Senior Executive Group (SEG).

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 (MC) and NATO Military bodies, the Digital Policy Committee (DPC), NATO Civil bodies, National Security Authorities (NSAs) and Designated Security Authorities (DSAs) are addressed in the NATO Security Policy. 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 4 – NATO CIS Security Documentation Structure

1. This “Primary Directive on CIS Security” is supported by a number of CIS (Cyber) Security directives and guidance documents addressing CIS Security management and CIS (Cyber) Security technical and implementation aspects. A collection of these and other security-related documents with Alliance-wide relevance is regularly provided by the NATO Office of Security. This “NOS 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 "NOS Roadmap" provides access to the following:

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

(b) contact information of NATO Security Authorities and other relevant security offices.

3. The "NOS Roadmap" is provided as an informational courtesy collection to NATO entities with a business interest. While the NOS undertakes reasonable efforts to keep the content accurate and as current as possible, the responsibility to have all relevant policy documents is solely with the cognizant stakeholder in its role as business (process) owner, implementer, contracting authority, operator, user, security management staff, or security accreditor.