COUNCIL OF THE EUROPEAN UNION

Brussels, 28 May 2014

10346/14

LIMITE

CSCI 10
CSC 120

NOTE

From :	The General Secretariat
To :	Delegations
Subject :	Information Assurance Security Guidelines on CIS Security Accreditation

Delegation will find attached the "Information Assurance Security Guidelines on CIS Security Accreditation" as approved by the Council Security Committee on 21 May 2014.

This page intentionally left blank

IA Security Guidelines on CIS Security Accreditation

IASG 1-01

This version replaces Doc. 8420/12 of 30 March 2012

TABLE OF CONTENTS

I. PURPOSE AND SCOPE

1. These guidelines, agreed by the Council Security Committee in accordance with Article 6(2) of the Council Security Rules (hereinafter 'CSR'), are designed to support implementation of the CSR.

2. The purpose of these guidelines is to describe the process and minimum activities to be considered when performing security accreditation of communication and information systems (CIS) handling EUCI.

3. The Council and the General Secretariat of the Council (GSC) will apply these security guidelines in their structures and CIS.

4. Member States should use security guidelines as a benchmark when EUCI is handled in national structures, including in national CIS.

5. EU agencies and bodies established under Title V, Chapter 2, of the TEU, Europol and Eurojust should use these security guidelines as a reference for implementing security rules in their own structures.

6. The CSR mandate that all CIS handling EUCI undergo a security accreditation process to obtain assurance that a sufficient level of protection of the EUCI and of the CIS has been achieved.

7. The Security Accreditation Authority (SAA) is responsible for establishing the security accreditation process and a supporting structure. The process must include at least the principles, roles and activities detailed in these guidelines.

8. These guidelines define:

   (a) the security accreditation process (definition, general principles, strategy, roles with responsibilities, statement and maintenance program. See section II);
   (b) minimum accreditation process activities and elements to consider during the CIS life cycle phases[1] (See section III).

[1] See Doc 16268/12 (IASP L: IA security policy on security throughout the CIS life cycle).

II. THE SECURITY ACCREDITATION PROCESS

II.1 Definition

9. A CIS security accreditation establishes the SAA confidence that the system security posture, with its related risk posture for the organisation, is sufficient to protect EUCI.

10. This confidence is based on evidence (e.g. risk analysis outcomes, testing results, etc) collected during the accreditation process and formalised in an accreditation statement stating the CIS accreditation decision with corresponding terms and conditions of validity.

11. The accreditation process is a framework defining potential activities to be performed and evidence to be collected to help the SAA in taking the most well founded decision whether to authorise the use of a CIS.

12. There are three possible outcomes of the accreditation process:

    (a) the SAA concludes that the level of protection of the EUCI and the CIS is sufficient, and that residual security deficiencies and related residual risks can be accepted. In that case, the SAA may grant an accreditation specifying the maximum classification level of the EUCI to be handled as well as potential corresponding terms and conditions such as the validity period of the accreditation;

    (b) the SAA concludes that the level of protection of the EUCI and the CIS is not fully sufficient but that the residual security deficiencies and related residual risks can be accepted taking into account that there are significant business needs that require the system to operate. In such a case, the SAA may issue an interim approval to operate (IATO) defining remedial actions to be implemented in a specified timeframe, so that the system will become accreditable. An IATO is not an accreditation, and its validity period must not exceed one year;

    (c) the SAA concludes that the level of protection of the EUCI and the CIS is insufficient and withholds or decides to withdraw an approval to operate or an accreditation until the security deficiencies are addressed.

II.2 General principles

13. The aim of the accreditation process must be a quality and compliance control of the CIS security posture with respect to the security obligations and constraints applicable to the organisation.

14. For any given system, the accreditation process must be in principle re-iterated every three years when all terms and conditions of the accreditation statement are continuously met.

15. The accreditation process must

(a) be included in the organisation's CIS project framework;
(b) be applied throughout the CIS life cycle;
(c) be commensurate with business risks;
(d) enforce SMART[2] activities objectives;
(e) define clear lines of accountability for roles;
(f) define agreed metrics for assessments and decisions;
(g) be as consistent as possible with that of cooperating parties.

16. The SAA should authorise conditional reuse of results from previous accreditation process activities (e.g. appropriate generic accredited (sub)systems can be defined and reused where relevant) in order to avoid duplication of effort.

II.3 System-specific accreditation strategy

17. The accreditation process, as described in sections II.1 and II.2, defines all the generic activities which could be performed during an accreditation.

18. When the process is applied to a particular CIS, or a partial evolution of a CIS, the SAA decides and records in a System-specific Accreditation Strategy (SAS) to what extent each activity must be performed and which outcomes are required. The aim of this strategy is to achieve a reasonable confidence while remaining cost effective and compliant with the organisation's expectations and obligations.

19. The SAS document follows the system throughout its entire life cycle. In particular the SAS will record:

(a) the list of retained accreditation process activities with rationale to shorten or remove some of them (such as CIS contexts, re-use of already security tested components (e.g. ESA[3] generic solutions), impact on business, available resources, etc);
(b) the maturity level for and specific outcomes and methods when performing activities;
(c) the documents to be produced;

[2] SMART : Specific, Measurable, Attainable, Relevant and Time-bound

(d) the actors, with assigned roles and hierarchy, who will be called upon to participate in the accreditation process;

(e) the outcomes of activities and discussions, acting as accreditation references on rationale for accreditation decisions.

20. To support IT management and resources planning, the SAA should define generic accreditation strategies for particular CIS contexts and security requirements (e.g. classification level of information, place of use, type of application, etc). These generic strategies must be coordinated with ESA generic solutions.

21. The SAS document should avoid redundancy and incorporate by reference the information already included in other system documents (e.g. USOR, SSRS, SecOPs or other project management documents).

II.4 Roles

22. The minimum roles include the business representative, the CIS representative and the SAA. Additional roles may be added by the SAA to increase the accuracy of accreditation activities.

23. Where a role is assumed by several actors accountability and delineation of responsibilities in the role must be clearly defined and a hierarchy established.

24. To avoid conflicts of interest the SAA will not assume any responsibility in other roles during the accreditation process. The business and CIS roles should be assumed by different actors.

25. The roles must collaborate in finding a secure solution which represents the best compromise between all organisation needs, obligations and priorities (e.g. budget, security, functionality, scheduling, etc).

BUSINESS REPRESENTATIVE

26. The business representative takes care of the interests of business users during accreditation. In particular this includes

(a) providing support to accreditation actors for accurate understanding of business needs;

(b) controlling that business needs and derived security objectives remain central during accreditation activities and decisions;

[3] ESA : Enterprise Security Architecture as defined in Doc 16268/12 (IASP L).

(c) approving any modification to the business needs and security objectives, should changes become mandatory to allow for accreditation.

CIS REPRESENTATIVE

27. The CIS representative is in charge of integrating accreditation concerns into the system throughout its life cycle.

28. The main actors assuming the role are mostly determined by the ongoing CIS life cycle phase. Whereas the project manager is an obvious candidate at the beginning of the project, the Information Assurance Operational Authority (IAOA) should progressively take the lead when security documents have to be written and accreditation maintenance activities are performed.

29. The CIS representative must ensure that the security solution integrates the recommendations expressed during the accreditation process. In particular this includes

(a) ensuring appropriate resources are available to support accreditation activities on the system;
(b) organising access to the system for security review and validation;
(c) updating security solution and documentation to reflect accreditation decisions.

SAA

30. The SAA is responsible for security accreditation. In particular this includes

(a) leading and coordinating the execution of the accreditation process;
(b) deciding, on the basis of inputs from all accreditation actors, on an appropriate accreditation statement for the system;
(c) managing the accreditation maintenance program.

31. Depending on the maturity level to be reached by the accreditation strategy, the SAA may ask for support by a security certifier and a security validator to perform certification and validation activities (see Par 64 - 68). These actors must have an appropriate expertise of CIS security issues and solutions, and be independent of the business and CIS actors.

32. When a CIS is shared with or amongst partners a Security Accreditation Board (SAB) or equivalent will be set up to fulfil the role of SAA.

II.5 Statement and documentation

33. The accreditation statement is the official document issued by the SAA to formalise the decision that a system is authorised to protect EUCI. The statement should include an executive summary with appropriate information for distribution to management stakeholders.

34. When an accreditation board has been set up the board, as SAA, issues the accreditation statement, based on Statement of Compliance (SoC) issued by participating SAA's board members. The SoC is an attestation that the CIS component(s) comply with the requirements for accreditation as defined in relevant security documents (e.g. SSRS, SecOPs, etc).

35. In principle the accreditation statement is classified R-UE/UE-R. When some elements included in the statement require a higher classification (e.g. accepted system deficiencies), it is recommended to put such elements into a separate, appropriately protected, document in order to preserve easy access by the stakeholders of the CIS to the accreditation statement.

36. The accreditation statement must contain the following information:

    (a) accreditation scope;
    (b) accreditation level;
    (c) accreditation validity period;
    (d) corresponding terms and conditions.

SCOPE

37. The scope precisely describes

    (a) the accredited system, with relevant identification data such as name, owning organisation and SAA, boundaries, etc;
    (b) the important CIS aspects influencing the system accreditation such as type of application, place of use, etc;
    (c) references to the set of documents supporting the accreditation decision.

38. The scope normally addresses a unique, specific CIS. The statement may also be generic when identical systems are (re)used in similar environments and/or have partial identical security requirements. In this case the statement must define explicitly the additional activities to be performed and aspects to take into account (e.g. specific physical security evaluation, (inter)connections, etc) when an instance of the generic CIS is put into operation.

LEVEL

39. The statement must unambiguously mention the maximum information classification authorised in the system, with additional elements of mode of operation and need to know when relevant.

40. To provide an accurate overview of the security objectives the statement must also mention the integrity and availability (and where appropriate authenticity and non-repudiation) levels offer by the system. The statement will as such clearly indicate how the CIS can be considered as a reliable tool, at the C-I-A levels, for supporting business processes.

VALIDITY PERIOD

41. Every statement will mention a maximum validity period for the accreditation; the criteria leading to the revocation of the validity period have to be documented in the terms and conditions.

TERMS AND CONDITIONS

42. The terms and conditions describe criteria underlying the accreditation statement. This includes

    (a) indicators to be fulfilled in order to preserve the confidence that the security posture is sustained and appropriately monitored;
    (b) indicators which, if met, lead to the review or even revocation of the accreditation statement.

43. The criteria will be defined by the SAA when performing the accreditation activities. As an exhaustive list can be rather difficult to build, the terms and conditions must always mention an action by default (e.g. immediate report to the IAOA) should an unexpected situation arise.

44. The statement must list all the documents which have to be considered as part of the accreditation process.

45. The minimum documents to be provided are

    (a) the SAS, reflecting in detail all the accreditation process activities that have been performed;
    (b) the USOR;

(c) the CIS residual risks statement;

(d) the SSRS;

(e) the SecOPs;

(f) the outcomes of the validation activity (see III.2) if any;

(g) the report of the certification activity (see III.2) including weaknesses, deficiencies and potential corrective actions.

II.6 Maintenance program

46. The SAA will manage a CIS security accreditation maintenance program to schedule (re)accreditation activities and provide to the management an ongoing overview of CIS security and risk postures in the organisation.

III. SECURITY ACCREDITATION PROCESS ACTIVITIES

47. Performing standardised activities helps ensure a consistent and repeatable application of the process and interpretation of the outcomes from system to system, providing stakeholders and partners with assurance that the security posture has been assessed through an approved set of activities.

48. The process and activities are aligned to the four CIS life cycle phases defined in IASP L. Each activity is described in terms of objective and minimum elements to consider. As for the CIS life cycle, accreditation activities are likely to undergo reviews and re-iterations.

III.1 Activities during the justification phase

49. The objective during this phase is to agree on an initial strategy amongst the accreditation actors.

50. This requires to correctly define the CIS security objectives, system scope and accreditation boundaries in accordance with the relevant policies, clearly stating the approval conditions and related schedule, level of effort, and resources required.

51. During this phase, the accreditation process must include at least the following activities:

(a) CIS registration;

(b) accreditation group setup;

(c) accreditation strategy definition.

CIS REGISTRATION

52. The CIS registration objective is to ensure that CIS undergoing an accreditation process receive the right support and advices for a smooth running of the accreditation activities throughout the CIS life cycle.

53. This activity must consider the following elements:

    (a) organisation security obligations and constraints as listed by the Information Assurance Authority (IAA);
    (b) assessment of the need for accreditation;
    (c) overview of the conditions to be satisfied to obtain and maintain an accreditation;
    (d) update of the list of all organisation's CIS, even those not planned to be accredited but already addressed in the IT plans.

ACCREDITATION GROUP SETUP

54. The accreditation group setup objective is to ease coordination of actions and decisions between the accreditation actors. The group is the place where accreditation issues should be first addressed and solved. The group is chaired by the SAA.

55. This activity must consider the following elements:

    (a) determination of accreditation actors;
    (b) group setup and definition of mandate;
    (c) available resources to perform the accreditation process.

ACCREDITATION STRATEGY DEFINITION.

56. The accreditation strategy definition objective is to produce the initial SAS.

57. This activity must consider the following elements:

    (a) review of the obligations and constraints influencing the potential security solution;
    (b) business security objectives to be implemented, as derived from USOR, organisation security risk analysis, etc;
    (c) available skills and security measures to implement the business security objectives;
    (d) refinement of activities to be performed;
    (e) accreditation strategy alignment with CIS project milestones (i.e. main engineering decisions, conditional procurement, etc)

DOCUMENTS TO BE PRODUCED

58. At the end of this phase the following documents will be available:

    (a) updated list of organisation's CIS;
    (b) SAS for the to be accredited CIS;
    (c) the accreditation group composition and mandate;
    (d) agreement(s) between SAA when an accreditation board has been set up.

III.2 Activities during the engineering phase

59. The objective during this phase is to produce an well founded accreditation statement.

60. This requires to analyse the system security at an appropriate level to get a reasonable confidence that a sufficient security posture has been implemented and can be sustained.

61. When decisions impacting further engineering tasks have to be taken on CIS components, partial accreditation may be performed on these components to confirm the acceptance of the engineering decisions.

62. The SAA will not supplant the system actors as long as the proposed security solution can be deemed as sufficient.

63. During this phase, the accreditation process must include at least the following activities:

    (a) certification of the security posture;
    (b) validation of the security measures implementation;
    (c) drafting of a potential accreditation decision;
    (d) accreditation decision.

CERTIFICATION OF THE SECURITY SOLUTION

64. The certification objective is the acceptance of the security documentation and solution for compliance against security obligations and organisation's risk governance.

65. This activity must consider the following elements:

    (a) review the security documentation and any security relevant documents of the CIS;
    (b) assess the compliance of CIS security solution against security obligations;
    (c) assess, starting from the security objectives up to the security measures, the rationale behind successive security choices;

(d) assess adequacy (in terms of strength and assurance) of proposed security measures for correct compliance with the security requirements;
(e) certify that the security documentation, the security solution, and the validation activity when performed, comply with the expected frameworks;
(f) coordinate, with the accreditation actors, modifications to the security solution, and when necessary business needs, to allow for final accreditation;
(g) confirm that the relation between the security solution and the corresponding residual risk statement is explained and correct.

VALIDATION OF SECURITY IMPLEMENTATION

66. The validation objective is to increase the confidence in the security solution by providing, for certification, additional proofs of effectiveness of the implemented security measures.

67. When validation is required, the SAA must

(a) define a validation framework (methods, tools and expected outcomes) for system security implementation validation;
(b) define mission statement for the validation activity;
(c) define system security testing, evaluation and inspection (STE&I) plans;
(d) ensure that validation outcomes are repeatable and do not only rely on security validators skills;

68. This activity must consider the following elements;

(a) perform the validation tasks as authorised by the validation framework;
(b) assess compliance of architectures and security solution with ESA principles;
(c) coordinate with the CIS representative milestones for validation of system or components thereof;
(d) report without delay evidences of unexpected deficiencies;
(e) confirm effectiveness of security measures;
(f) propose potential improvements if any.

DRAFTING OF A POTENTIAL ACCREDITATION DECISION

69. The objective of this activity is to produce a draft accreditation statement for endorsement by the SAA.

70. This activity must consider the following elements:

(a) maximum acceptable residual risks;
(b) compliance with CIS security objectives. If not, rationale to accept non-compliance must be explained;
(c) assembly of the accreditation documentation data set;
(d) review by the accreditation representatives of the proposed potential accreditation statement.

71. Within this step, the business and CIS representatives may express in the executive summary of the accreditation statement(s) any concerns they have with the proposed accreditation decision.

ACCREDITATION DECISION

72. The objective of this activity is to publish the accreditation statement endorsed by the SAA.

73. This activity must consider the following elements:

(a) consensus with the business representative;
(b) rationale to choose a particular accreditation statement;
(c) decision by the SAA on an accreditation statement;
(d) acceptance by the business and CIS representatives of the obligations mentioned in the terms and conditions.
(e) acceptance by the business representatives of the CIS residual risks.

DOCUMENTS TO BE PRODUCED

74. At the end of this phase the accreditation statement will be signed and distributed by the SAA to the relevant stakeholders.

III.3 Activities during the sustainment and disposal phases

75. The objective during these phases is to monitor that the approved security posture and maximum level of risk are preserved.

76. The results of monitoring activities are continuously reported to the SAA in the form of status reports to decide if accreditation terms and conditions are met and system continued operation is still acceptable.

77. The SAA should put in place a common accreditation monitoring program for all systems within the organisation to ease exchange and correlation of security events.

78. Priority for accreditation monitoring is given to

(a) controls that are often modified or have been identified as ineffective to some degree;
(b) accreditation elements whose confidence is difficult to quantify.

79. During this phase, the accreditation process must include at least the following activities:

(a) system monitoring to ensure correct sustainment and disposal of (components of) the CIS;
(b) monitoring of the accreditation assumptions underlying the accreditation statement.

SYSTEM MONITORING

80. The system monitoring objective(s) is to confirm that the security posture remains valid.

81. This activity must at least consider the following elements:

(a) assess the way business users are using the system;
(b) nature and recurrence of security tasks to be performed on the system;
(c) check if security controls continue to be effective;
(d) updated security documents, monitoring reports content and recurrence;
(e) change and configuration managements;
(f) when a CIS is to be withdrawn ensure approved procedures are performed and reports drafted.

ASSUMPTIONS MONITORING

82. The assumption monitoring objective is to confirm that elements underlying the choices of security requirements and corresponding security measure are still valid.

83. This activity must at least consider the following elements:

(a) assess the organisation obligation and constraints;
(b) changes in the organisation's missions, risk landscape, business processes;
(c) assess risk assessment components (i.e. threat evolution, products strength and assurance requirements, new vulnerabilities, etc);
(d) changes in tolerance for previously accepted risks.

DOCUMENTS TO BE PRODUCED

84. As long as the CIS is in use, the following documents will be updated

(a) monitoring reports, leading to the appropriate review of SAS activities in order to guaranty coherence between the system security posture and its security documentation;

(b) continuous assessment of the security posture and risk level;

(c) CIS components disposal reports.