077768/EU XXIV. GP
Eingelangt am 30/03/12

COUNCIL OF THE EUROPEAN UNION

Brussels, 30 March 2012

8420/12

CSCI 12
CSC 21

NOTE

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

1. The Council Decision on the security rules for protecting EU classified information[1]1 states that "The Security Committee may agree at its level security guidelines to supplement or support this Decision and any security policies approved by the Council." (cf. Article 6(2)).

2. The CSC approved the attached Information Assurance Security Guidelines on CIS Security Accreditation on 28 March 2012.

---

[1] Council Decision 2011/292/EU, OJ L 141 of 27.5.2011, p. 17.

This page intentionally left blank

IA Security Guidelines on CIS Security Accreditation

IASG 1-01

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 CSR require accreditation for all communications and information systems handling EUCI of any level in electronic form (CIS).

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

4. When EU classified information is handled in national structures, including national CIS, the Member States will use these security guidelines as a benchmark.

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. These guidelines describe the steps to be followed for accreditation of CIS. The process outlined here is not normative but indicative and should be tailored by the Security Accreditation Authority (SAA) depending on the nature of the information being handled by the CIS to be accredited, the environment in which it operates and the expected protection needs for the information and hence for the CIS. The thoroughness and level of detail of the accreditation process - the Security Accreditation Strategy - is thus defined by the estimated level of risk specific to the CIS being accredited.

7. Lists in these guidelines are not exhaustive. The details of what items in the respective lists are needed for accrediting a specific CIS are set by the SAAs involved.

II. SECURITY ACCREDITATION

8. Accreditation is the process used to obtain an assurance that appropriate security measures have been implemented and that a sufficient level of protection of the EUCI and of the CIS has been achieved in accordance with the Council Security Rules.

9. The accreditation process for CIS is a key component of the overall objective of the Council Security Rules of reducing the risks of running a CIS in a manner which is cost effective, proportional to and adequate for the volume of the information it handles, the likelihood of a compromise of its security and the potential impact of such incidents.

10. The overall approach to accrediting any proposed communication and information system must as a rule follow the process outlined below.

11. As depicted in Figure 1, the security accreditation process is initiated by a trigger event, the most common being a request to the CIS owner for a new communication and information system intended to handle classified information. Other events could be changes of significant nature to the CIS, a changed level of threat or risk in the operating environment of a legacy CIS, a change in the regulatory framework, a breach of security, or a need of the CIS business owner to bring the security measures of a CIS up to higher standards.

12. The security accreditation process requires some information to be already available before it can be implemented. User Security Operational Requirements (USOR) must be available and the CIS design, including the planned security features, must be known up front in order to reach a first estimate of the degree of protection required by the CIS being accredited.

13. The accreditation process consists of a series of steps, the outcome of each of which is recorded as part of the Accreditation Data Set (ADS) needed by the SAA to reach a decision. The order of the steps outlined below is logical but not necessarily chronological.

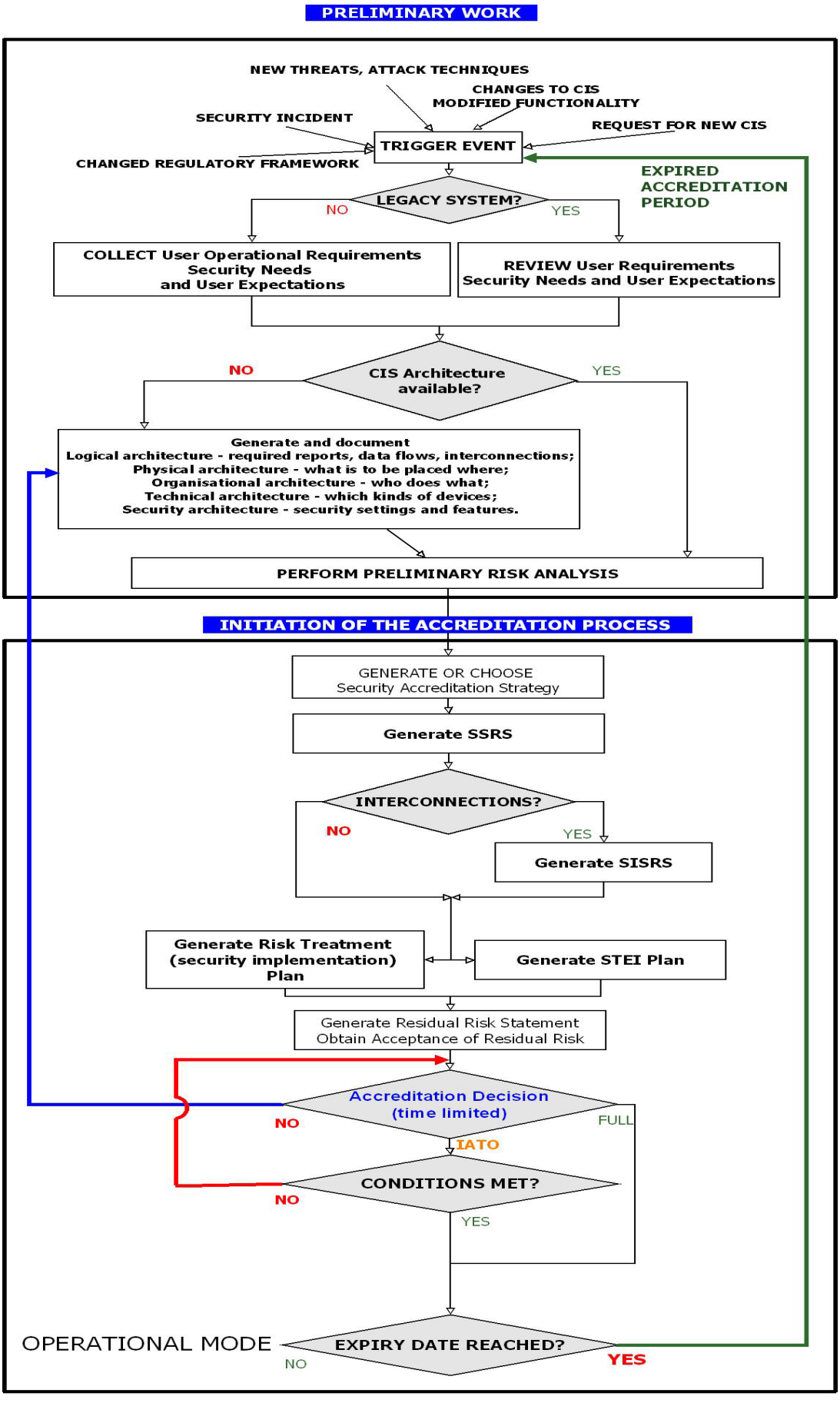
PRELIMINARY WORK
NEW THREATS, ATTACK TECHNIQUES
CHANGES TO CIS
MODIFIED FUNCTIONALITY
SECURITY INCIDENT
REQUEST FOR NEW CIS
TRIGGER EVENT
CHANGED REGULATORY FRAMEWORK
EXPIRED
ACCREDITATION
PERIOD
LEGACY SYSTEM?
NO
YES
COLLECT User Operational Requirements
Security Needs
and User Expectations
REVIEW User Requirements
Security Needs and User Expectations
NO
CIS Architecture
available?
YES
Generate and document
Logical architecture - required reports, data flows, interconnections;
Physical architecture - what is to be placed where;
Organisational architecture - who does what;
Technical architecture - which kinds of devices;
Security architecture - security settings and features.
PERFORM PRELIMINARY RISK ANALYSIS
INITIATION OF THE ACCREDITATION PROCESS
GENERATE OR CHOOSE
Security Accreditation Strategy
Generate SSRS
INTERCONNECTIONS?
NO
YES
Generate SISRS
Generate Risk Treatment
(security implementation)
Plan
Generate STEI Plan
Generate Residual Risk Statement
Obtain Acceptance of Residual Risk
Accreditation Decision
(time limited)
NO
FULL
IATO
CONDITIONS MET?
NO
YES
OPERATIONAL MODE
EXPIRY DATE REACHED?
NO
YES

Figure 1

II.1 User Security Operational Requirements

14. The security needs for the CIS in question must be collected, based on the input of users as to their requirements and expectations[1]. A set of User Security Operational Requirements with as much detail as possible is generated to provide the basis for further work. The outcome should therefore be documented as a USOR statement which is validated by the CIS business owner.

15. For legacy CIS, the original architecture may not have been built to such specifications[2]. Creation of a document describing the user expectations of the system at the time of (re-) accreditation is strongly recommended; see also below section II.12.

16. Such a list of user security requirements includes at least:

    (a) the security mode of operation;
    (b) the expected highest classification level of information to be handled and volumes, if possible sorted by degree of confidentiality;
    (c) the logical and physical environment in which the CIS is to be run;
    (d) the user requirements for availability, integrity of information and other domains of information security;
    (e) roles of users as well as of required support personnel;
    (f) interconnection needs; and
    (g) constraints and the resulting risks accepted by the CIS business owner according to pre-established criteria.

17. The USOR collected at the start of a project should not be considered indefinitely immutable, especially when the development, design and running phases cover significant periods of time so that technological solutions which were not available at start of work may be introduced, or the threat scenario may change during the CIS lifecycle.

18. While not in the direct scope of these security guidelines, the required and expected functional and technical features of the planned CIS are also recorded in documentation available to the SAA (see below paragraph 57).

[1] "musts" and "wants" etc.
[2] e.g. no user requirements were formally defined

II.2 CIS Design and Architecture

19. Based on the User Security Operational Requirements, the high level design of the CIS is defined which includes:

    (a) the proposed physical and geographical location(s);
    (b) the human resources needed to use and support the CIS;
    (c) the main active hardware and software components;
    (d) the methods to provide connectivity;
    (e) the security measures to be built into and the logical structure of the proposed CIS;
    (f) training needs, organisational changes, etc..

20. This directly defines the boundaries of what is to be accredited, and by implication specifies which types and severity of subsequent changes to the CIS will trigger its re-accreditation.

21. The documentation describing the planned or running CIS may have various names: system architecture, design, functional specifications, technical specifications and so on and is validated by the CIS business owner.

22. For the purpose of accreditation, information is needed as to how the proposed design meets the user requirements and expectations regarding:

    (a) Functional architecture - user interface, reports, features and services provided;
    (b) Logical architecture - data flows, interconnections;
    (c) Physical architecture - what is to be placed where;
    (d) Organisational architecture - who does what;
    (e) Technical architecture - which kind of device;
    (f) Security architecture - security settings and features;
    (g) Training needs, organisational changes etc.; and
    (h) Constraints: security policies and guidelines, regulatory, legal, financial or user requirements which must be met.

II.3 Risk Analysis

23. "Risk" means the potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact.

24. The CIS business owner must be consulted to establish the level of risk which is acceptable; see also paragraph 38.

25. A risk analysis is also a prerequisite for establishing a correspondence between security measures and levels of risk exposure. Risk assessment, in complex situations, is necessarily an iterative process. It is therefore often difficult to obtain an exact measure of the security risks and threats at the start of their life cycle. In such situations, the organisation tasked with building the CIS, in collaboration with the CIS business owner, may carry out an initial, high level step of an iterative risk assessment process to estimate the expected risk level of the CIS.

26. This analysis must therefore determine the estimated impact of disruptions on the basic security domains: availability, integrity, confidentiality of the information, as well as extensions thereof: the authenticity and non-repudiability of messaging or other transactions performed by the CIS on the information it handles.

27. The initial or preliminary risk analysis identifies:

- the criticality of the CIS to the organisation;
- the vulnerabilities inherent to the CIS as designed;
- the threat scenario to which the CIS will be exposed;
- the resulting levels of risk:- the risk scenario;
- the maximum classification level of the information which may be processed; and
- the mode of operation intended for the system.

28. The architecture of the prototype CIS then needs to be examined in greater detail. Such a study may reveal the need to make changes to the design to treat the risks which have been identified. The initial study may also reveal that the CIS can or should be viewed as being made up of different security subunits[3]. These subunits may be exposed to different risk levels so that, in order to simplify the work needed to achieve and maintain CIS security without losing required functionality, different sets of security countermeasures can be implemented.

29. For running CIS the above-mentioned study can often be omitted and a system-specific security requirements statement directly generated. The organisation tasked with building and/or running the CIS may also agree with the SAA that this preliminary risk analysis may be omitted for new CIS and proceed directly to detailed risk assessment.

II.4 Security Accreditation Process

30. Based on the information collected, the SAA draws up and implements a security accreditation strategy (SAS) for the CIS. See also section II.5.

31. Further, the SAA:

    (a) Consults, as needed, security experts, other experts and advisers, in order to be able to justify the accreditation decision taken; and

    (b) based on the evidence produced, issues the accreditation statement specifying the type of accreditation, interim approval to operate or withholding of approval of the proposed CIS.

32. The Accreditation Statement is thus the final document produced in the accreditation process.

II.5 Security Accreditation Strategy

33. The security accreditation strategy defines

    (a) the level of detail of the processes described in these guidelines and which steps are necessary;

    (b) the security indicators (milestones[4]) which should be achieved;

    (c) what needs to be documented as accreditation data set (ADS);

[3] a section of the CIS with a uniform set of security requirements different from those of other subunits.

[4] Measurable or demonstrable achievements of meeting the requirements

(d) the roles and actors involved in the accreditation process for the CIS;

(e) which levels of accreditation as described in paragraph 60 of these guidelines can eventually be achieved;

and includes requirements for:

(f) collecting, organising and analysing information relevant to CIS security;

(g) applying a risk management framework;

(h) security testing, evaluation and inspection[5]; and

(i) periodically analysing and assessing the security posture of the CIS.

34. The choice of type and the design of the SAS is up to the SAA.

35. The strategy can be system-specific or generic if the latter type is applicable to the CIS requiring accreditation. The result of the strategy can be a security accreditation report to justify the issuing of a security accreditation statement.

36. Generic SAS can be used e.g. to describe the security risks and requirements for a common component such as a workstation which is to be attached to a CIS handling EUCI. They can also cover types of CIS. In such situations, the generic SAS may be supplemented by an incremental SAS for those risks to which the particular CIS is exposed beyond and above the ones covered by the generic SAS.

II.6 Risk Assessment

37. Depending on the risk levels estimated in the initial risk analysis, more specific and detailed documentation is then produced, as a rule in the form of an SSRS.

38. The CIS business owner must set criteria to establish what level of risk is acceptable.

39. In-depth analysis of the CIS using the risk management methodology chosen by the organisation in question is needed in order to develop the SSRS, which the SAA examines and validates. The risk analysis takes into consideration synergy effects which may increase or decrease the overall risk level. If the CIS has cells of different security levels, it may be easier to treat each cell separately. A practical approach can be to first create an SSRS for each security cell and/or combine them to form an overall SSRS for the CIS. A key principle in developing the SSRS is that all components which are covered by the SSRS must be under the control of the organisation to which the SAA belongs.

[5] e.g. production of a "statement of compliance"

40. Interconnections of a CIS to other CIS or networks which fall within the remit of different SAAs require that the different SAAs develop a common Security Accreditation Strategy and jointly produce the final Accreditation Statement.

41. The SSRS is the main collection of security requirements against which the CIS is evaluated during the process of accreditation. It is based on a risk assessment using principles of risk management in a standardised process which takes into account the impact, likelihood and ease of detection of the event leading to the risk[6].

42. Risks which satisfy the criteria of being acceptable as in paragraph 38 are not further considered except by special request of the CIS business owner. They must be, however, included in the residual risk acceptance statement.

43. The SSRS is also the basis for producing a system-specific security-implementation plan as well as for a System Security Testing Evaluation and Inspection plan (STEI plan). The STEI plan will be developed alongside the system functional specifications and system security-implementation plan. It will include checks to ensure that the CIS is built securely and that the requirements of the SSRS have been met. Additionally, the STEI plan may include functionality and quality checks to determine whether the CIS meets user expectations and functional needs.

44. An SSRS is based on a snapshot of the security environment in which the CIS operates and may require modification as described later.

II.7 Risk Treatment Plan

45. A system-specific Risk Treatment Plan is then generated and describes the security measures and methods selected to enhance the reliability and security of the CIS and reduce the risk to the level considered acceptable by the CIS Business Owner.

46. Initial risk treatment plans drawn up from best-in-class collections of security vulnerabilities, threats and countermeasures should, however, be enhanced and customised by the design, development and implementation teams, in consultation with security experts and the CIS business owner.

[6] e.g. using methods of "Failure Mode and Effect Analysis"

47. Risk treatment required by the plan may involve either, all, or combinations of:

- avoiding or eliminating the risk by removing the vulnerability or the threat;
- mitigating or reducing the risk by introducing workarounds or compensating measures;
- transferring the risk[7].

48. As required by the CSR, best practices should be adhered to and implemented. If standard builds are to be used, references must be made both to the documentation of such builds, as well as to the results of their testing.

49. Deviations from best practices must be documented and a justification for them provided in the plan.

50. The plan will include details of planned TEMPEST protective measures, cryptographic protection, crypto material management, etc., as applicable and required for the CIS under consideration.

II.8 System Security Testing Evaluation and Inspection

51. This involves using the STEI plan described above for estimating whether the requirements of the SSRS are reflected in the CIS.

52. While initial testing is typically done in a development set-up by the development team, release testing of the CIS is preferably done by an independent entity not previously involved in its design and development, in a dedicated test environment which closely emulates the production system.

53. For the purposes of accreditation, security testing will determine whether the security countermeasures required in the SSRS have been correctly implemented.

54. The results of testing and evaluation are reported by the security accreditation review team and constitute, or are appended to, the statement of residual risk as applicable.

[7] Acceptance of risk is handled by the statement of acceptance of residual risk

II.9 Residual Risk Management Plan

55. A formal Statement of Acceptance of Residual Risk and/or a Residual Risk Management Plan is therefore needed to document which risks were accepted by the business up front, which risks remain after treatment and why they are not eliminated.

56. The CIS business owner signs this Statement of Acceptance of Residual Risk. In certain circumstances, a different authority may be designated as Security Risk Owner whereupon the latter must accept the residual risks for the CIS.

II.10 Accreditation Data Set

57. The ADS will include documentation on the measures which will be taken to protect the CIS from inadvertent or malicious attack - the Network Defence programme for the CIS .

58. With the proviso that it is up to the SAA to determine what is required, a good Accreditation Data Set (ADS) should consist of:

- User Security Operational Requirements;
- System Architecture and Design;
- the results of the initial Security Risk Analysis;
- Criteria for accepting risk;
- Security Accreditation Strategy;
- the System-specific Security Requirement Statement (SSRS);
- System-specific Interconnection Security Requirement Statements (SISRS) when applicable
- the Risk Treatment Plan;
- the System Security Testing Evaluation and Inspection plan (STEI plan);
- the results of testing by the security accreditation review team, e.g. as a SIVR - system inspection and verification report;
- Security Operating Procedures (SECOPS) which should include:
    - crypto plans as applicable;

- disaster recovery and contingency[8] plans;
- plans and schedules for review of the performance of deployed security measures;
- Network Defence measures including security monitoring and incident response;
- Security requirements for internal and external personnel involved in the development and maintenance of the CIS e.g. capability and maturity ratings for actors involved in creating and maintaining the CIS, number of dedicated persons required, certifications held, security clearance;
- Security requirements for components e.g. crypto policy, ITSEC, ISO15408 (common criteria) levels;

– A Statement of Acceptance of Residual Risk or Residual Risk Management Plan.

59. Configuration details also need to be documented in order to determine what will be considered a change request not relevant to security and what change requests may require re-evaluation of the accreditation status.

II.11 Accreditation Statement

60. On the basis of the available data and documentation, there are three possible outcomes:

(a) the SAA can conclude that the residual security deficiencies do not prevent the CIS going into operation in the short term. In such a situation a conditional interim approval to operate may be issued with the requirement that the remaining issues be addressed and the CIS resubmitted for accreditation within a specified time period;

(b) the SAA can conclude that the CIS meets all expectations and requirements and issue a time-limited accreditation statement; or

(c) the SAA may find the CIS does not meet the requirements and withhold accreditation until the deficiencies are addressed.

61. The accreditation decision will be documented in this statement based on the evidence collected and will define the maximum classification level of the information that may be handled in a CIS as well as the corresponding limitations and conditions for the validity of the accreditation being granted.

[8] Contingency plans are often called business continuity plans; they come into operation during a loss of service to enable limited service to be maintained until the full service is restored by the disaster recovery process. They must include scenarios when accepted risks cause incidents.

62. The accreditation statement specifies the time limit after which the accreditation or interim approval to operate expires.

63. The accreditation statement also defines the types and degree of changes to the CIS components or to the environment it operates in which trigger full or partial renewed accreditation.

64. Before changes are made to the CIS and/or when important new threats are discovered, the IA operational authority must consult the SAA to evaluate their impact in order to determine whether re-accreditation is needed or not.

II.12 Legacy CIS

65. Since the accreditation statement is time-limited and since changes in technology or the threat scenario can force renewed accreditation, the process of accrediting running CIS is different in that the premises on which the accreditation was given must be reviewed.

66. As mentioned in paragraph 15, legacy CIS may not have all required documentation.

67. A comparison between the current and original sets of user security requirements and expectations therefore needs to be performed.

68. The original design must also be compared to the current one to determine whether security-significant changes have been made.

69. Similarly the risk-analysis exercises may need to be repeated to determine whether the SSRS needs revision.

70. Based on the results of the above, a new ADS and consequently a new accreditation statement may be needed. If no security impact is determined by the above exercise, the accreditation may be prolonged by a new statement or by an annex to the old one.

71. Further, the analysis may reveal that in order to achieve renewed accreditation, modifications are needed to the CIS which may be so extensive that the CIS needs replacement or upgrade.

Annex 1

Roles and Actors involved in CIS Accreditation

1. The roles described below are not necessarily descriptions of different physical persons - one person may fulfil several roles as long as there is no conflict of interest.

Users

2. Users must communicate their needs clearly, and express constraints and required features such as ease of use, timing and budget, which may affect the course of the accreditation process. They are key to developing the User Security Operational Requirements documentation. The owner of the information processed by any communication and information system is the user community. Accreditation is thus performed by the SAA in the name of the users, based on their input as regards functional and security requirements.

CIS business owner

3. The CIS business owner[9] represents the interests of the entity or entities who will benefit from the functionality provided by the CIS, and is thus in a position to define which level of risk is acceptable.

4. The CIS business owner is required to sign the statement of acceptance of the documented residual risks identified by the accreditation process.

Development Team

5. The team must develop the design and architecture of the CIS and ensure that it meets user requirements and expectations. Its members include the Information Assurance Operational Authority (IA OA). It create prototypes and test-beds necessary prior to developing the final CIS. The IA OA, which is responsible for drafting the SSRS, must ensure maintenance of security and service levels during the operational lifetime of a CIS. The development team builds the CIS and ensures that it is documented to enable the support teams and the users to operate, maintain and use the CIS during its lifetime.

[9] system owner

Support Team

6. The support personnel must establish whether the proposed CIS is capable of being maintained and monitored so as to be able to meet the service levels expected by the users. They include the IA operational authority, which is responsible for implementing the security measures of the CIS and following up on any unexpected disturbances as well as for delivering any CIS-specific training required.

CIS Owner

7. The CIS Owner or head of operations, the project or program manager in charge of developing CIS, is responsible for the co-ordination of security work on the CIS under study and co-ordinates the activities of the above two teams.

8. The two teams are typically involved in defining the system-specific documentation, based on their expertise and knowledge of the state of the art for CIS of the type being developed. The initial draft of the STEI plan is thus drawn up jointly by the development team and the support team under the leadership of the CIS owner.

Security Experts

9. Experts on information assurance policy and operation, personnel security and physical security will review, advise and assist in refining the security documentation to ensure that it conforms to existing policy and regulations, besides meeting user expectations and requirements. Such experts are typically the IA Operational Authority, the IA Authority, the Tempest Authority, and the Security Office. They will also be involved in ensuring that the STEI plan includes security checks of sufficient strength to be able to check conformity of the CIS to the SSRS.

Other Experts and Advisors

10. In the above process, the advice of legal, financial, or other experts should also be requested as applicable when defining the SSRS, e.g. to determine the legal and regulatory constraints in which it operates.

Security Accreditation Review Team

11. This team checks the compliance of the CIS to user the USOR and SSRS. Their expertise may also be requested in developing the STEI plan as they are its primary users. User functional requirements may be part of the overall plan for system testing but are not crucial to the accreditation process. The team issues an opinion of whether the CIS as implemented has fulfilled the security requirements in a document which also describes the residual risks of the CIS reviewed.

Security Accreditation Authority

12. The role of the SAA is described in the Council Security Regulations, Annex IV. The SAA defines the SAS, consults subject matter experts as needed, evaluates and documents the evidence collected and issues the accreditation decision.

Annex 1

Abbreviations

ADS	Accreditation Data Set
CIS	Communications and Information System: cf.: Article 10 (2) of the CSR
CSR	Council Security Rules
IA OA	Information Assurance Operational Authority - defined in CSR
IATO	Interim approval to operate
SAA	Security Accreditation Authority
SAS	Security Accreditation Strategy
SECOPS	Security Operating Procedures
SISRS	System-specific Interconnection Security Requirements Statement
SIVR	Security Inspection and Validation Report
SSRS	System-specific Security Requirements Statement
STEI	Security Test, Evaluation and Inspection
TEMPEST	A short name referring to investigation and studies of compromising emanations of CIS components
USOR	User Security Operational Requirements