**COUNCIL OF
THE EUROPEAN UNION**

**Brussels, 26 November 2013
(OR. en)**

16678/13

**CSC 160
CSCI 65
SAP 5**

COVER NOTE

From:	The General Secretariat of the Council
To:	Delegations
Subject:	General framework for managing the security accreditation of communication and information systems (CIS)

1. Delegations will find attached the new general framework for managing the security accreditation of GSC communication and information services (CIS), approved by the GSC's Security Accreditation Authority on 26 November 2013.

2. The framework is used for implementing Article 10(4) and relevant parts of Annex IV of the Council Decision of 23 September 2013 on the security rules for protecting EU classified information. It was endorsed by the Council's Security Accreditation Board (SAB) on 21 November 2013.

Encl.: 1

This page intentionally left blank

GENERAL SECRETARIAT OF THE

COUNCIL OF THE EUROPEAN UNION

General framework for managing the security accreditation of communication and information systems (CIS)

26 November 2013

This page intentionally left blank

TABLE OF CONTENTS

TABLE OF FIGURES

1 Introduction

This framework aims to structure security accreditation within the General Secretariat of the Council based on good governance throughout the process[1]. The framework only deals with security accreditation aspects; it does not address CIS project management.

The GSC's Security Accreditation Authority (SAA) is responsible for drawing up and implementing/maintaining the framework (see Article 3 (1) of Decision 184/10 of the Secretary-General) [REF. 7]. The SAA is supported by the SAA Support Team in that task.

The Security Accreditation Board (SAB) has agreed to use this framework as a basis for accrediting systems within the remit of both the GSC and external entities. It may also be used as a benchmark by Member States for accrediting national systems handling EU classified information.
The SAA will update this framework as necessary. All updates will be communicated to the Security Accreditation Board (SAB).

1.1 Definition and scope of security accreditation

Definition
Accreditation is the method used to obtain an assurance that all 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.

Scope
The Council Security Rules (CSR - REF. 1) require that all communication and information systems handling EUCI at any level in electronic form, including systems internal to the GSC or operated by the GSC within the remit of both the GSC and the Member States, undergo an accreditation process. CIS security accreditation is a key component of the overall objective of the CSR of reducing the risks of running a classified CIS in a cost-effective manner commensurate with the volume of classified information handled, the likelihood and potential impact of compromise of the security of the information it handles. Security accreditation activities take place throughout the life cycle of classified systems.

The scope of accreditation of a CIS encompasses the following:

(a) the CIS infrastructure in its environment(s);
(b) the operational services run over this infrastructure;
(c) where appropriate, interconnections to other CIS.

[1] This document cancels and replaces the previous framework endorsed by the then C-SAP in April 2010.

The SAA may decide to apply the processes outlined in this framework to any system handling sensitive unclassified information whenever warranted by a risk analysis and relevant user security operational requirements.

1.2 Framework for managing the security accreditation process for CIS

The framework covers the following:

(a) Description of the general framework for security accreditation and its constituent elements (section 2)
(b) Security Accreditation Cycle (section 3)
(c) Security risks assessment/management (section 4)
(d) Security Accreditation Strategy (section 5)
(e) Security measures implementation (section 6)
(f) Security tests, evaluation and inspections (section 7)
(g) Security Inspection and Verification Report (section 8)
(h) Statements of compliance (section 9)
(i) Security Accreditation Report/Security Accreditation Statement (section 10)
(j) Security Accreditation Programme (section 11)
(k) Security Accreditation Data Management (section 12).

1.3 References

The framework has been drawn up based *inter alia* on the references listed in Annex 1. For a detailed glossary of applicable terminology, see ISO/IEC 27005 [REF 5.].

1.4 Actors in the accreditation process

Annex 2 contains an overview of roles and responsibilities of the actors involved in the accreditation process.

2 General framework for security accreditation and its constituent elements

2.1 Constituent elements of the framework

The general framework covers the following:

(a) **security risks assessment and follow-up**: ensuring that risks are identified and subsequently accepted or treated using an agreed security risk management process;

(b) **measuring the security level**: ensuring that the necessary tests, evaluations and inspections are performed using agreed methods and procedures;

(c) **monitoring the security posture**: ensuring that the actual security level of a CIS is accurate and monitored/measured using agreed indicators;

(d) **cooperating**: ensuring that processes are in place to ensure cooperation between all security actors on on-going accreditation issues;

(e) **communicating**: regular reporting to relevant stakeholders about security accreditation issues;

(f) **programming security accreditation activities**.

2.2 Cyclical nature of the accreditation process

The accreditation process consists of different phases:

(a) **assessment of the system security justification**, in accordance with inter alia paragraphs 50-52 of IASG 1-01 (IA security guidelines on CIS security accreditation) [REF. 2, doc. 8420/12 - currently being updated];

(b) a complete **security risks assessment** for each CIS (and focused security risks re-assessments as required);

(c) **security measures implementation**;

(d) a complete **security verification** (and focused **security verification** tests, evaluations, inspections);

(e) a complete security **residual risks review**;

(f) preparation of the **Security Accreditation Report (SAR) / Statement (SAS);**

(g) **approval of the SAR/SAS by the GSC's SAA or the joint Security Accreditation Board (SAB)**.

The security documents resulting from each of these activities are subject to validation by the competent SAA before the next step of the cycle can be initiated. Further details are given in the following sections.

Changes to any classified CIS are to be handled in accordance with Change Control Board (CCB) procedures. The SAA Support Team will contribute to the process of validating change requests, where relevant on the basis of an assessment of the impact of the change request on the overall security posture of the system, to be provided upon request by the Information Assurance Operational Authority (IAOA) and/or the Security Office (where changes to the physical environment are introduced).

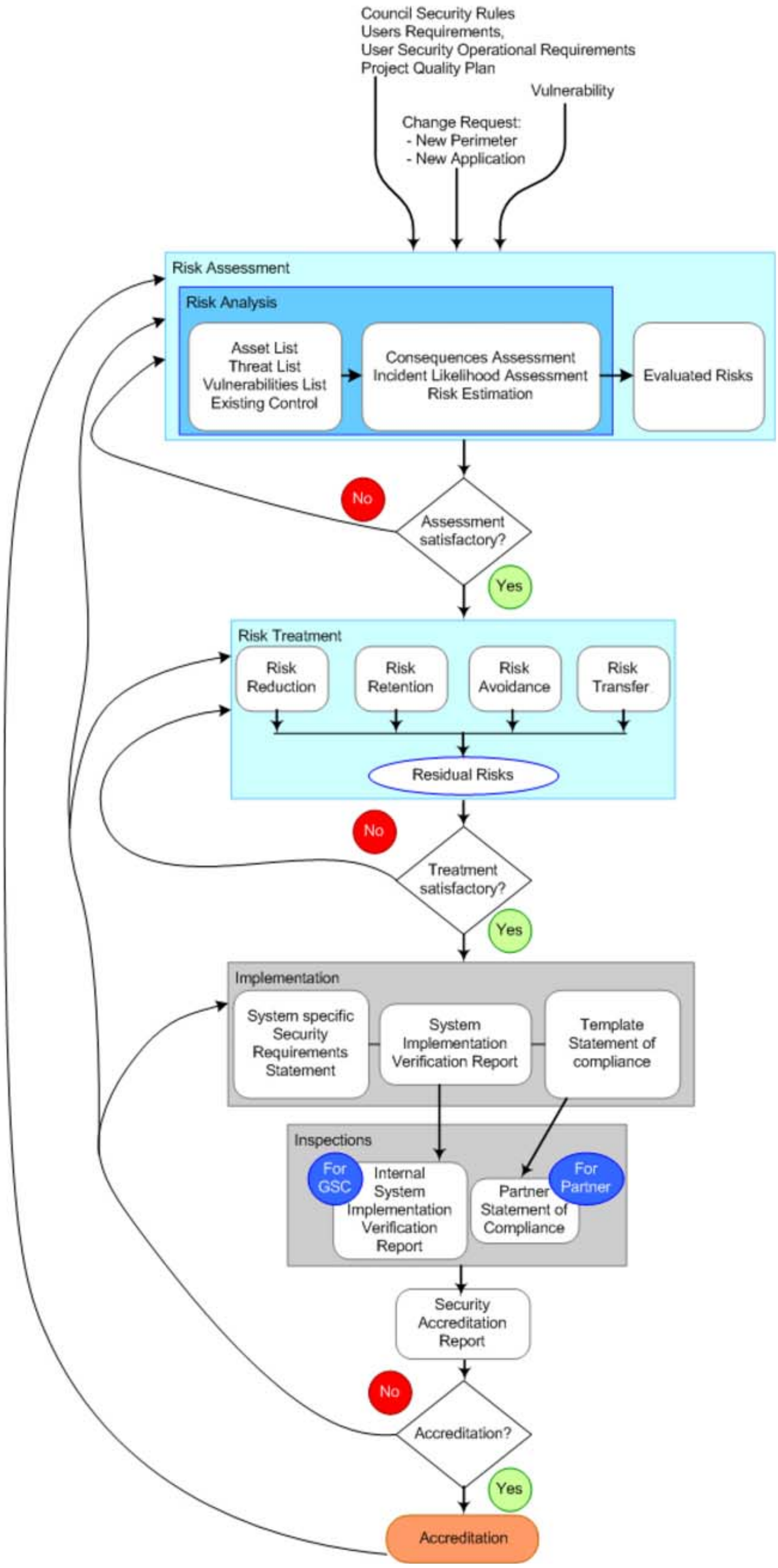

Figure 1 - Illustration of the security accreditation process

Note: In the event of no decision to accredit the system, a return to the risk treatment and risk assessment phases is not necessarily required.

3 Security Accreditation Cycle

The various steps of the accreditation process and how they link into the post-accreditation steps are set out in the figure below:

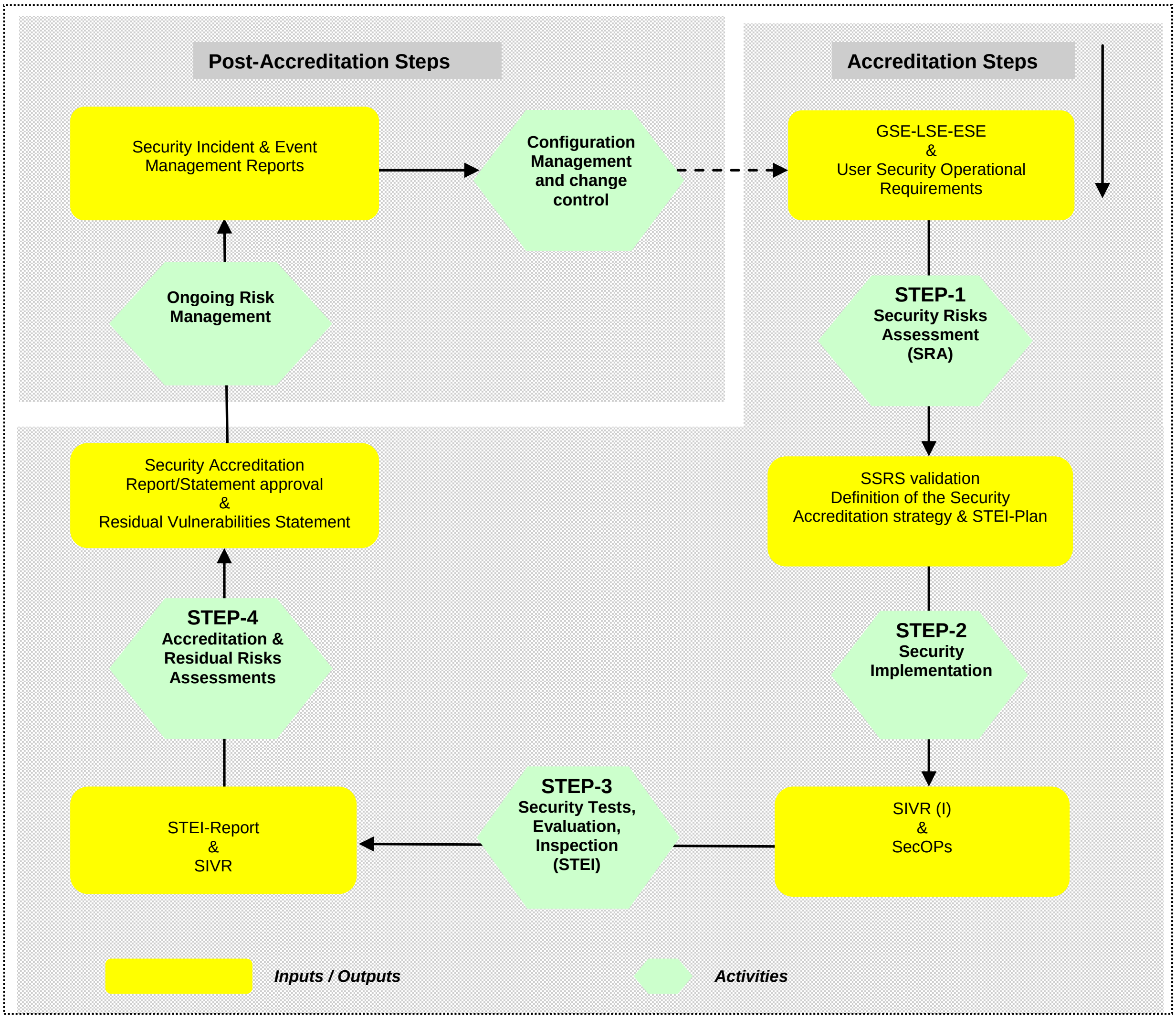
Post-Accreditation Steps
Accreditation Steps
Security Incident & Event Management Reports
Configuration Management and change control
GSE-LSE-ESE & User Security Operational Requirements
Ongoing Risk Management
STEP-1 Security Risks Assessment (SRA)
Security Accreditation Report/Statement approval & Residual Vulnerabilities Statement
SSRS validation Definition of the Security Accreditation strategy & STEI-Plan
STEP-4 Accreditation & Residual Risks Assessments
STEP-2 Security Implementation
STEP-3 Security Tests, Evaluation, Inspection (STEI)
STEI-Report & SIVR
SIVR (I) & SecOPs
Inputs / Outputs
Activities

Figure 2 - Security accreditation cycle

The security accreditation cycle may be implemented in three variants:

- long cycle: building or significantly re-building the security of a CIS
- short cycle: mitigating residual risks
- ad hoc cycle: approving a (new) application or sub-system.

4 Security risks assessment/management

4.1 General principles

Security risk assessment is the first step in the accreditation process. Security risks will be analysed and managed in conformity with ISO/IEC 27005: 2011. The approach toward security risks is adapted rapidly, periodically or on an ad hoc basis as and when the risk environment evolves (i.e. threat sources, threats, vulnerabilities of assets, the value of assets, and potential impacts of incidents).

4.2 Risk Management process

4.2.1 In the absence of a GSC Information Security Management System (ISMS), the risk management process will be structured as follows:

(a) context establishment, on the basis of a Users' Security Operational Requirements (USOR) Statement (see template in Annex 4) and an analysis of high level CIS design;

(b) risk assessment on the basis of the definition of organisational risk tolerance (risk "appetite") agreed by GSC senior management or the SAB as appropriate, with clear valuation dimensions, an explicit definition of relevant business assets, and an ISO-based threat catalogue. As regards the identification of vulnerabilities, the standard list presented in ISO may be used;

(c) risk treatment (mitigation/acceptance/avoidance/transfer);

(d) risk communication;

(e) risk monitoring and review.

4.2.2 Risks are formulated in terms of:

(a) asset/information value, threats, vulnerabilities;

(b) consequences / impact (in terms of availability, integrity, confidentiality and cost);

(c) likelihood.

From the combination of the parameters mentioned above, a risk level can be derived.

4.2.3 The risk management model will enable action to be taken, whenever possible, on one or more risk parameters. These include:

- implementing additional **controls** (corrective measures) or reinforcing existing ones;
- correcting **vulnerabilities** of support assets**;**

- reducing the level of **threat** by acting on their origins or pre-requisites;
- reducing the exposure level of **assets**.

4.2.4 In the cyclical accreditation approach, the following types of Security Risk Assessment will be performed:

(a) [SRA-1] Full Security Risk Analysis - typically made at the early stages of the CIS project and re-iterated every three years as part of the SSRS drafting/review programme;

(b) [SRA-2] Residual Risk Analysis - typically made before granting a security approval to the CIS;

(c) [SRA-3] Ad hoc Security Risk Analysis - typically made in case of significant change requests to the CIS (new application, extension to a new site, etc.).

4.2.5. Because all actors involved in the CIS life-cycle need to contribute to security risk management, security risk analysis is performed as a collective, multi-disciplinary process led by the Information Assurance Operational Authority (DG A CIS), based on input from the following:

(a) the Security Office, which will assess all elements related to physical security (GSE[2]/ LSE[3]);

(b) the Information Assurance Authority;

(c) the SAA;

(d) users, through the provision of USOR (and - if possible - participation in the SRA process);

(e) the sensitive CIS manager (SCISM).

[2] The general security environment (GSE) relates to the physical security measures surrounding the location where the system is installed (e.g. external fences and gates). The general security environment shall be defined and the corresponding responsibilities clearly identified.

[3] The local security environment (LSE) relates to the non-technical security measures surrounding the office areas where components of the system are located (server rooms, user workstation areas, hubs, etc.). It shall be defined and the corresponding responsibilities clearly identified.

5 Security Accreditation Strategy

Depending on the nature and classification level of the information being handled by the CIS to be accredited, organisational risk appetite, the environment in which it operates and the expected protection needs for the information, the accreditation cycle can be tailored appropriately. The SAA will take a decision in the interest of both security and cost-effectiveness.

A distinction may be made between two categories, based on their classification level:

- Low classified CIS (RESTREINT UE - EU RESTRICTED)
  - medium physical security and access control constraints;
  - medium crypto constraints;
- High classified CIS (CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/ EU SECRET)
  - strong physical security and access control constraints,
  - TEMPEST constraints;
  - strong crypto constraints;
  - registration / accountability.

For each system, based on the information gathered during the initial risk analysis phase and on User Operational Security Requirements (USOR), the SAA will determine a Security Accreditation Strategy, which will define:

(a) the level of detail of the process described in this document: which steps are necessary;
(b) the security indicators (milestones) to be achieved;
(c) what needs to be documented as the accreditation data set (ADS - see Annex 3)

and include requirements for:

(d) security testing, evaluation and inspection;
(e) periodically analysing and assessing the security posture of the CIS and
(f) interconnection needs.

In the case of legacy systems, prior to a regular review of the security documentation, USOR must be produced under the auspices of DG A CIS project management, supported by the Information Assurance Operational Authority and by the SAA Support Team, if this has not been part of the initial procedure, so as to enable the risk assessment phase to be structured on the basis of clear business requirements.

On the basis of the multi-disciplinary risk analysis and the security accreditation strategy, more specific and detailed documentation will be produced by the Information Assurance Operational Authority, as a rule in the form of an SSRS (System-Specific Security Requirements Statement) and/or SISRS (System-specific Interconnection Security Requirements Statement). The SSRS is the most important collection of security requirements against which the CIS will be evaluated during the accreditation process. The structure and content of an SSRS document are laid down in the IA Security Guidelines on System-specific Security Requirements Statements (IASG 1-02) (doc. 14305/13). The SSRS forms the basis for drafting:

- the Security Operating Procedures (SecOPs) which will be prepared in two parts: a technical explaining in detail the actual security implementation in the final system and a concise, user-friendly general section setting out in simple plain language the roles and responsibilities of users;
- the system-specific sections of the Security Inspection and Verification Report (SIVR).

Clear mapping must be guaranteed between the risks identified during the risk analysis phase and the proposed corrective measures, the performance of which must be assessed against relevant key indicators.

6 Security measures implementation

The SSRS requirements and the technical provisions of the SecOPs, the SIVR and the TSoC are the basis for security measures implementation, and for the system Security Testing Evaluation and Inspection plan (STEI plan). Cost-effective technical and non-technical counter-measures must be in place to manage the assessed risk.

The choice of counter-measures is usually a compromise between operational constraints, technical requirements, legal requirements, budgetary constraints and available personnel. The security counter-measures must be organised so as to enable defence-in-depth as described in applicable information assurance policies and guidelines. The counter-measures have to be positioned in all three security environments (GSE/LSE/ESE).

DG A CIS project management is responsible for implementing the security measures.

7 Security tests, evaluations and inspections (STEI)

The Council Security Rules state (Annex IV - paragraph 47 (e)) that "the SAA is responsible for: checking implementation of security measures in relation to the CIS by undertaking or sponsoring security assessments, inspections or reviews".

This section of the document lays down the conditions related to the security testing, evaluation and inspection of CIS subject to accreditation.

7.1 STEI Objectives

The STEI process assesses the security of platform, application software, and network devices of a system, mainly but not only by checks of:

- physical Security at General Security Environment (GSE) perimeter [*]
- physical Security at Local Security Environment (LSE) perimeter [*]
- network security
- server and workstation security
- application security.

The aim of the STEI-process is to produce the deliverables needed to:

- have a clear view of vulnerabilities and to be able to assess residual risks;
- verify if all requirements of the SSRS are met by appropriate and sufficient counter-measures and are performing as expected;
- verify if applicable information assurance policy requirements are met.

7.2 STEI Types

Security test, evaluation and inspection activities can be of the following types:

- [STEI-1] initial full STEI performed after implementation of security measures; this includes the electronic, local and general security environments
- [STEI-2] specific security checking to control implementation of corrective measures identified in a previous initial (STEI-1) or an ad hoc STEI campaign
- [ad hoc STEI] STEI activities made as part of accreditation maintenance activities or as part of an inspection campaign covering the classified CIS perimeter in a horizontal manner.

[*] For the parts of classified systems housed outside GSC premises, GSE/LSE assessments are outside the scope of the GSC assessment teams.

7.3 STEI Approach

The ISO 27000 series standard should be used to organise security requirements and STEI controls.

The STEI is evidence-based. Any evidence found is verifiable. It is based on samples of information available during the STEI period.

7.4 STEI Requirements

To effectively conduct testing activities, the following documents must be available to the testing team: SSRS, SIVR, SecOPs, the inventory of assets, the system's technical manual and the installation manual.

8 Security Inspection and Verification Report

To ease the security accreditation process and to facilitate the implementation of the Security requirements, a Security Inspection and Verification Report (SIVR) is to be completed by the STEI contributors. The SIVR contains information on

- risks identified during the risk analysis
- corrective measures to be implemented to mitigate the risks identified during the risk analysis
- the implementation status of the corrective measures
- residual risks evaluation after the implementation and the verification of the corrective measures.

The SIVR is transmitted to the SAA support team together with any other inspection reports made by the STEI Team.

The SIVR may be used to review the Template SOC to be distributed to relevant partners.

The SIVR, along with any other inspection report made by the STEI team, is used by the SAA to assess the security posture of the inspected system.

9 Statements of compliance

Entities with a system node or interconnection have to complete a "Statement of Compliance" (SoC). SoCs are an essential component of the accreditation process, as they provide all system partners with a tool to assess the security posture of a Point of Presence/system node or interconnection. They play an essential role in collectively managing risks.

The following apply to SoCs:

- template SoCs will be provided by the GSC SAA to all system partners each time a new SSRS is approved. When the SAB is the SAA for the system concerned, the template SoC for Points of Presence (PoP) or interconnections (ICN) is validated by the SAB;
- when the SAB is the SAA for the system concerned, the corresponding SoC must be validated by the SAB;
- in order to be valid, a SoC must contain the following:
  - complete PoP and interconnections (ICN) identification (name, location, type of (secure) area) with a comprehensive partner network diagram of PoP actual implementation including possible ICNs to partner systems;
  - full contact details (name, first name, telephone, e-mail);
  - summary inspection information (date, place, inspecting authority);
  - for PoP SoC an authorised signature and stamp by the relevant NSA;
  - summary risk assessment information in the event of non-compliance with a specific requirement;
  - for ICN a copy of the "national accreditation certificate for the protection of EUCI" signed and stamped by the relevant SAA;
- SoCs are valid for three years;
- if no valid SoC is available for a PoP or interconnection, this PoP or interconnection cannot be included in an Interim Approval to Operate (IATO) or accreditation for the system concerned. In such cases, information will only be provided electronically up to LIMITE level to the partner concerned, and vice versa;
- six months prior to the expiry of a SoC, the GSC SAA Support Team sends a letter to the partner(s) concerned to remind them of the expiry deadline [*];
- when a new template SoC is drafted following approval of a new SSRS, previously received SoCs remain valid until the end of their three year period, but SoC renewal has to be performed on the basis of the most recent template;

[*] In some cases, this task is delegated to the system SCISM.

- SoCs must be renewed in the event of (i) a significant capability upgrade; (ii) discovery of a significant vulnerability; or (iii) discovery of a significant incident or breach of security.

Note: The template SoC will not necessarily be classified, but once it has been completed, it should be classified at least R-UE/EU-R. Transmission of the SoCs to the GSC SAA Support Team should be done via the dedicated GSC SAA mailbox in electronic format (encrypted) and hard copy (through registered mail) according to procedures for the transmission of EUCI.

10 Security Accreditation Report (SAR)/Security Accreditation Statement (SAR-S)

Based on the result of the first phases of the security accreditation process, as documented in the SIVR and STEI reports, the SAA Support Team will prepare the security accreditation report (SAR). The SAA organises appropriate consultations in the event of problems appearing during analysis of the SIVR and STEI reports. Each SAR is circulated to the other stakeholders for review, comments and inputs. Once consolidated, the SAR and SAR-S are approved either by the GSC SAA or by the joint Security Accreditation Board (SAB). Divergences of opinion between stakeholders may be recorded in the SAR.

The security accreditation statement (SAR-S) determines the terms and conditions of the accreditation. It will refer to the security accreditation report. Once the security accreditation statement has been approved, the system is accredited.

Accreditation will apply to systems with an accepted risk level, in the light of the organisational risk tolerance agreed by GSC senior management or the SAB as appropriate, even if the security posture is not yet optimal. With a view to optimising or maintaining the security posture of accredited systems, the SAR will list action to be taken in the short, medium and long term, as well as concomitant resource requirements.

If a system has not reached accreditable status in the light of available evidence or if significant residual risks cannot be accepted, the SAR will also list the conditions to be fulfilled within a specific timeline for the system to reach accreditable status. In such cases, the system may receive an interim approval to operate (IATO).

If an IATO is granted, responsibility for the security posture of the system is shared between all system partners.

11 Annual Security Accreditation Programme

11.1 Objectives and scope

Activities related to the accreditation process are described in an annual accreditation programme drafted jointly by relevant GSC security actors (IAA, SO, IAOA, DG A CIS, SAA support team). The programme is approved by the SAA.

The annual accreditation programme will include activities required to plan and organise accreditation activities for all relevant systems and to provide the necessary resources as such activities can be conducted in a timely and efficient manner. With a view to resource allocation and defining the programme priorities, it is important to anticipate the necessary activities for existing systems and to retain sufficient capabilities to address new CIS and ad hoc security needs.

Any outcome of an accreditation activity (Security risk assessment report, SSRS, STEI report, SAR, etc.) is reviewed, approved and formally released to the SAA and other interested entities.

11.2 Management

The procedure for managing the accreditation programme is

(a) the programme is drawn up annually (year N). For year N:

i. the programme should be established by the beginning of the last quarter of year N-1;

ii. the programme should be validated by the SAA by December of year N-1;

iii. the programme should be reviewed quarterly and updated as necessary;

(b) reports on the implementation status of the accreditation programme are submitted following every review to the competent SAA. In this context, indicators to monitor how well the programme is functioning include:

i. where relevant, an assessment by the heads of relevant entities of the capacity of teams to implement the programme (sizing, availability, etc.);

ii. conformity with the programme and planning;

iii. feedback from the programme sponsor (SAA), security expert teams, project / system teams.

12 Security Accreditation Data Management

12.1 Data management indicators

Accreditation data are managed throughout the accreditation cycle. Data are grouped in sixteen categories (indicators).

Data management is based on the following indicators:

(a) indicator 1 - Description and Status: The purpose of the CIS is accurately described, its application and network configuration properly identified and its security and operational status kept up-to-date;

(b) indicator 2 - Organisation: The organisation of the CIS is appropriately established and personnel designated for key roles, especially the SCISM;

(c) indicator 3 - Security Documentation: The security documentation exists, is up-to-date and accessible;

(d) indicator 4 - Security Steps: The position of the CIS in the accreditation cycle is known;

(e) indicator 5 - Security Assessments: A record exists of past security assessment and next assessments are planned;

(f) indicator 6 - Users: Users of the CIS are identified as well as their level of security awareness and training;

(g) indicator 7 - Administrators: Administrators of the CIS are identified as well as their level of clearance, security awareness and training;

(h) indicator 8 - Residual Vulnerabilities: Residual vulnerabilities are recorded, identified, assessed and treated;

(i) indicator 9 - Corrective Measures: Corrective measures are recorded, planned and their implementation monitored;

(j) indicator 10 - Residual Risks: Residual Risks are identified, assessed and managed/accepted;

(k) indicator 11 - Physical Environment: The physical environment where the CIS is deployed is identified and its security level controlled;

(l) indicator 12 - Points of Presence: When the CIS is deployed in sites not under the control of the GSC, those "points of presence" are identified and their security posture controlled;

(m) indicator 13 - Interconnections: Interconnections to the CIS are identified, described and controlled;

(n) indicator 14 - Import / Export: Data flows from and to the CIS, and associated techniques are identified and controlled;

(o) indicator 15 - Change Management: Changes to the configuration of the CIS are controlled;

(p) indicator 16 - Incident Management: Security incidents on the CIS are appropriately logged and treated.

Most of the above indicators will be collectively managed through the SAA dashboard collaborative tool (“WebSAA”), according to an agreed approach.

12.2 Security Bulletin

The SAA Support Team organises regular IT Security Risks/Vulnerabilities Reviews (ISRR) at working level to provide GSC security decision-makers and actors with a Security Bulletin giving an overview of the security posture of classified CIS and of the state of implementation of the Security Accreditation Programme.

The Security Bulletin includes concise information concerning:

- the accreditation status of the systems;
- the vulnerability and risk status;
- the planned corrective measures.

The security bulletin is for GSC senior management. For CIS accredited by the SAB, the SAB will receive a similar bulletin.

The ISRRs are without prejudice to existing CIS project management groups.

````````````````````````````````````````
````````````````````````````````````````

ANNEX 1

References

[REF 1.] Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU) (OJ L 274 of 15 October 2013)

[REF 2.] GSC Information Assurance policies and security guidelines, in particular the following:

- Information Assurance Security Policy on Security throughout the CIS life cycle (IASP L) (doc. 16268/12)
- Information Assurance Security Guidelines on CIS Security Accreditation (IASG 1-01) (doc. 8420/12 - currently being updated)
- Information Assurance Security Guidelines on System-specific Security Requirement Statement (SSRS) (IASG 1-02) (doc. 14305/13)
- Information Assurance Security Guidelines on Security Operating Procedures (SecOPs) (IASG 1-03) (doc. 14306/13)

[REF 3.] ISO/IEC 27001 - Information security management systems - requirements

[REF 4.] ISO/IEC 27002 - Code of practice for information security management

[REF 5.] ISO/IEC 27005 - Information security risk management

[REF 6.] ISO 19011 - Guidelines for quality and/or environmental systems auditing

[REF 7.] Decision 184/10 of the Secretary-General of the Council on the designation and tasks of the Security Accreditation Authority

[REF 8.] Decision 185/10 of the Secretary-General of the Council on the designation and tasks of the Sensitive Communication and Information Systems Coordinator

[REF 9.] Decision 181/10 of the Secretary-General of the Council on the tasks of the Security Office

[REF 10.] Decision 183/10 of the Secretary-General of the Council on the designation and tasks of the Information Assurance Operational Authority and the Crypto Distribution Authority

[REF 11.] Decision 45/13 of the Secretary-General of the Council on the designation, mission and tasks of the GSC's Information Assurance Authority.

ANNEX 2

Roles and responsibilities of the various actors involved in the accreditation process

1. The Information Assurance Authority (IAA)

The mission and tasks of the GSC IAA are set out in Decision 45/13 of the Secretary-General of the Council on the designation, mission and tasks of the GSC's Information Assurance Authority [REF 11].

The IAA ensures inter alia the following functions in the security accreditation area:

- provide guidance on the security of information and on implementing and maintaining the security of CIS, in particular CIS handling EUCI;
- develop IA security policies and security guidelines […];
- provide advice on IA policy to the Security Accreditation Authority (SAA) and contribute to accreditation boards and panels, and support the security accreditation process by reviewing relevant security documentation (e.g. SSRS, SecOPs, etc.);
- ensure that security products to be used in communication and information systems are qualified in accordance with the relevant IA policy.

2. DG A CIS

DG A CIS provides the physical equipment, software and communications necessary to establish and maintain CIS operated by the GSC. Its duties include amongst others:

- developing, implementing and maintaining CIS on the basis of user requirements, and other requirements listed in the various security documents;
- parameterisation and administration of CIS;
- maintaining sensitive equipment if necessary after they have been configured by the security administration teams for CIS;
- managing procurement procedures and contracts;
- financial planning and execution (including inventory management);
- providing technical support for security actors in the context of tests/evaluations of security products.

3. CIS users

The CIS user community is responsible for defining the requirements and expectations related to the security needs for the CIS undergoing an accreditation process. This implies that a set of User Security Operational Requirements is generated that 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 and integrity of information and other aspects of information security;
(e) roles of users as well as of required support personnel;
(f) interconnection needs; and constraints and the resulting risks accepted by the CIS system owner according to pre-established criteria.

4. Security Office (SO)

The terms of reference of the GSC SO are set out in Decision 181/10 of the Secretary-General of the Council on the tasks of the Security Office [REF 9]. In the area of security accreditation, the SO plays a role inter alia in security risk assessment/management, maintaining a database of personnel clearances, and conducting physical security inspections of areas where EUCI are handled (both the general and local security environments - GSE/LSE).

5. Information Assurance Operational Authority

The Security of Sensitive CIS unit at DGA CIS acts as the GSC's Information Assurance Operational Authority under Decision 183/10 of the Secretary-General of the Council on the designation and tasks of the Information Assurance Operational Authority and the Crypto Distribution Authority [REF 10]. As IA Operational Authority, it ensures inter alia the following functions:

- drawing up the following security documentation required for the accreditation process: (i) the System-Specific Security Requirements Statement (SSRS) (risk analysis and appropriate countermeasures); (ii) the SecOPs; (iii) the IT security parameter guidelines; (iv) the SIVR, and (v) the TSoC;
- drawing up other relevant operational security documentation as appropriate;
- participating in selecting and testing system-specific technical security measures, devices and software, supervise their implementation and ensure that they are securely installed, configured and maintained in accordance with applicable security documentation;

- performing checks of the ESE[4];
- ensuring network defence;
- ensuring the security administration of systems (crypto, Tempest, etc.);
- network defence.

6. Security Accreditation Authority (SAA) and SAA Support Team

The tasks of the GSC SAA are set out in Decision 184/10 of the Secretary-General of the Council on the designation and tasks of the Security Accreditation Authority (see REF. 7). Its duties include inter alia the following:

- drawing up and implementing a general framework for managing the security accreditation process for CIS;
- drawing up an annual work programme for security accreditation related activities, in liaison with the IA Operational Authority;
- determining the Security Accreditation Strategy for a CIS;
- examining and approving security-related documentation;
- contributing to security risks analysis;
- verifying implementation of security measures in relation to a CIS by undertaking or sponsoring security assessments, tests and inspections;
- approving physical and personnel security requirements with regard to a CIS;
- approving the interconnection of a CIS to other CIS, where relevant as part of a joint approval process;
- providing Security Accreditation Reports containing recommendations for a statement of approval or accreditation for a CIS to handle EUCI to a defined level of classification in its operational environment;
- monitoring at regular intervals the security posture of CIS;
- chairing the joint Security Accreditation Board (SAB) meetings and providing support and assistance to SAB members.

7. Member States and other partners - Security Accreditation Board (SAB)

Joint Security Accreditation Board (SAB)

Formal accreditation of systems within the remit of both the GSC SAA and Member States is carried out by a joint Security Accreditation Board in order to ensure full involvement of the Member states in the process, as defined in Annex IV, par. 50, of the Council Security Rules.

[4] The ESE checks relate to the electronic counter-measures put in place within the boundaries of the system.

As a general rule, the SAB meets three times per year (February/March, June/July, October/November).

Statements of compliance

Member States or other entities with nodes on a system under an accreditation process need to provide statements of compliance (SoCs) for points of presence (PoPs) or for interconnections (ICNs), on the basis of templates provided by the GSC SAA.

8. Sensitive CIS Manager

The Sensitive CIS Manager (SCISM) is responsible for the operation of controls and special security features of the CIS he manages. This responsibility extends throughout the life cycle of the SCIS from the concept stage to final disposal, and implies that he has responsibility for (i) all security measures designed as part of the SCIS, after delegation by the SCIS Coordinator; (ii) the preparation and implementation of the Security Operating Procedures (SecOPs); (iii) the specification of security standards and practices, and (iv) for organising the security awareness training for users. The SCISM acts on behalf of the IAOA.

ANNEX 3

Accreditation Data Set

Document/file	**Department responsible for drafting/approval**
User Security Operational Requirements, listing at least (i) the security mode of operation, (ii) the expected highest classification level of information to be handled and volumes, if possible sorted by degree of confidentiality, (iii) the user requirements for availability, integrity of information and other domains of information security, (iv) roles of business users as well as of required support personnel, (v) interconnection needs, and (vi) constraints put forward by the CIS system owner;	user community, supported by CIS project management
Information related to the design of the system: • data models (e.g. entity relationship diagram) and data formats; • protocols used; • components and connections/dependencies between them (at least those involved in the processing of EUCI); • interfaces; • platforms, frameworks, middleware and operating systems used within the CIS; • user management and access control mechanism; • interactions with users and external systems (e.g. use case diagrams); • data flows (at least those involving EUCI handled within the system); • physical and deployment diagrams showing network topology, hardware and associated CIS components; • links with business requirements (e.g. connection between business use cases and system use cases)	DG A CIS
System maintenance documentation	DG A CIS
The results of the initial Security Risk Assessment	IAOA, on the basis of input of the other actors involved in the process
Criteria for accepting risk	management, input from IAOA, SAA

Security Accreditation Strategy	SAA
The System-specific Security Requirement Statement (SSRS), both the initial version and the updated version following STEI activities	drafted by IAOA, validated by SAA
The Risk Treatment Plan	IAOA
The System Security Testing Evaluation and Inspection plan (STEI plan)	VASSI team at IAOA
The results of testing by the security accreditation review team, e.g. as a SIVR - system inspection and verification report	VASSI team at IAOA + Security Office + Information Assurance Authority
Security Operating Procedures (SecOPs), which should include: 1) the list of counter-measures for the risks identified in the SSRS; 2) crypto plans as applicable; 3) disaster recovery and contingency plans; 4) plans and schedules for review of the performance of deployed security measures; 5) network defence measures including security monitoring and incident response; 6) 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; 7) security requirements for components e.g. ITSEC, ISO15408 (= common criteria) levels 8) user SecOPs to be signed off by users	IAOA IAOA DG A CIS + BCP IAOA IAOA (NDC) DG A CIS + IAOA + Security Office Information Assurance Authority IAOA /SCISM
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	analysis by SAA support team, where relevant on the basis of an assessment by IAOA of the impact of the change on the security posture of the system
The Security Accreditation Report with the list of residual risks	SAA support team

ANNEX 4

Template for a User Security Operational Requirements (USOR) statement

User Security Operational Requirements for *<<specify_name>>*

Purpose

This document describes the basic security characteristics (User Security Operational Requirements) of the above-mentioned CIS. It does not replace the SSRS nor risk assessment, nor any other analytical document. The security needs are based on the input of users as to their requirements and expectations. The documents contains as much detail as possible to provide the basis for further work. The outcome is validated by the CIS business owner signed at the end of the document. The document will be updated along the life cycle of the project when more information is acquired. The requirements will be refined after their validation in the next phases of the project and after confronting them with project constraints (resources, time, quality required).

Project Identification

Basic information identifying the project.

Business Context of the CIS

The basic business context of the CIS is described in the Excel file that comes with this template.

Threat Sources

Within the business context of the CIS, the business owner is invited to identify the main threat sources, and possibly qualify them by a threat level after the following scale. The threat sources can be external but also internal to the organisation.

Confidentiality Needs

The table below defines the confidentiality needs as seen by the business stakeholders. It applies to the information processed by the CIS. The confidentiality can also apply to the information about the fact that certain business information is handled inside the system. The needs are not defined per each piece of information but rather aggregated for the 'types of information' to be handled within the system. The objective of this paragraph is to document the proportion and the scope of confidentiality needs for the CIS rather than to replace a detailed risk assessment.

Availability Needs

The table presents the availability needs defined by the business users. It applies to the information, processes and/or services expected from the CIS aggregated in such a way that the reader can see the highest, lowest and typical needs and the proportions between them.

Auditability Needs

In this document, the word auditability is meant as the ability of a CIS to collect, manage and safeguard pieces of evidence of operations it has done, for investigation purposes. It is related to traceability of transactions, registration of logs, time stamping, authenticity of information and non-repudiation. As for the integrity of information, it is considered in this document as *"the property of safeguarding the accuracy and completeness of information and assets"*[5]. The protection of integrity during transmission is usually given for free as a side effect of the encryption means. This is the reason why, in this document, it is assumed that the integrity during transmission of information is ensured as soon as the information has been transmitted in encrypted form. Nevertheless, in some cases, the business owner may have stronger requirements such as the need for information authenticity (i.e.: proof of the origin of the information exchange) or, still stronger, the need for non-repudiation of information transactions (i.e.: "*the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied*"[6]).

[5] CSR

[6] CSR

Interconnection Needs

This paragraph contains all interconnection needs identified in the current state of the project.

Other Non-functional Requirements

This paragraph contains all non functional requirements that have impact on security and that are known at the current stage of the project. Example non-functional needs contain, but are not limited to: technology constraints, resilience, usability, scalability, maintainability, testability, extensibility and so on.

Other Comments

Give any information that may help the reader to gain an accurate and relevant vision of requirements for the CIS.

____

Business owner signature

ANNEX 5

List of abbreviations

ADS	Accreditation Data Set
BIC	Bureau des Informations Classifiées (Classified Information Office)
CCB	Change Control Board
CIA	Confidentiality - Integrity - Availability
CIS	Communication and Information Systems
CM	Corrective Measure
DGA CIS	Directorate in charge of CIS at DG A
ESE	Electronic Security Environment
EU	European Union
EUCI	European Union Classified Information
GSC	General Secretariat of the Council
GSE	General Security Environment
IAA	Information Assurance Authority
IAOA	Information Assurance Operational Authority
IATO	Interim Approval To Operate
ICN	Interconnection of Network
IMPEX	Import / Export
ISMS	Information Security Management System
ISO	International Standard Organisation
ISSR	IT Security Risks/Vulnerabilities Review
IT	Information Technology
LSE	Local Security Environment
NAA	National Accreditation Authority
POP	Point of Presence
SAA	Security Accreditation Authority
SAB	Security Accreditation Board
SAMS	Security Accreditation Management System
SAR	Security Accreditation Report
SAR-S	Security Accreditation Statement
SCISM	Sensitive Communications and Information System Manager
SecOPs	Security Operating Procedures
SG	Secretary-General
SIVR	Security Implementation and Verification Report
SMI	Security measures Implementation
SO	Security Office
SoC	Statement of Compliance
SRA	Security Risk Assessment
SSCIS	Security of Sensitive CIS Unit
SSRS	System-specific Security Requirements Statement
SISRS	System Interconnection Security Requirements Statement
STEI-P	Security Test, Evaluation and Inspection Plan
STEI-R	Security Test, Evaluation and Inspection Report
USOR	User Security Operational Requirements statement
VASSI	Visite d'Aptitude à la Sécurité des Systèmes d'Information