COUNCIL OF THE EUROPEAN UNION

Brussels, 14 November 2013

16086/13

CSCI 62
CSC 143

NOTE

From :	The General Secretariat
To :	Delegations
Subject :	Information Assurance Security Guidelines on Security Operating Procedures (SecOPs)

1. The Council Decision on the security rules for protecting EU classified information[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 Security Operating Procedures (SecOPs) on 14 November 2013.

[1] Council Decision 2013/488/EU of 23 September 2013, OJ L 274, 15.10.2013, p. 1

This page intentionally left blank

IA Security Guidelines on Security Operating Procedures (SecOPs)

IASG 1-03

This version replaces ISP 200 of February 2003

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 minimum mandatory structure and content of the Security Operating Procedures (SecOPs) allowing each stakeholder involved in system security management to easily find the relevant information to perform his or her duties.

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. The Council Security Rules (CSR) mandate the development of CIS security documentation, in particular the SecOPs, which are to be developed under the responsibility of the system Information Assurance Operational Authority (IAOA).

7. These guidelines must be used by the IAOA to develop SecOPs explaining to the security stakeholders how the security requirements stated in the System-specific Security Requirement Statement (SSRS) are implemented and sustained.

8. As stated in the IASP L[2], the SecOPs are developed during the engineering phase of a particular CIS and are a precise description of the components (either personnel, processes or technologies) chosen to implement the security requirements stated in the SSRS.

9. The description of these components constitutes the reference for the security conformance testing before a security accreditation statement can be given for the system. The SecOPs are then periodically updated as required by the conditions outlined in its maintenance chapter.

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

10. The SecOPs are the management document of the security posture of the system. When approved by the SAA as part of the security accreditation process, the SecOPs form a binding security agreement between the IAOA and the system security stakeholders on how the security of the CIS must be sustained.

11. In principle the SecOPs are classified R-UE/UE-R. When some elements included in the SecOPs require a higher classification, it is recommended to put such elements into a separate document in order to preserve easy access by the stakeholders of the CIS to the main parts of the SecOPs.

II. SECURITY OPERATING PROCEDURES

II.1 SecOPs layout

12. The SecOPs are structured as following:

    (a) SecOPs executive summary;
    (b) SecOPs scope;
    (c) CIS security components;
    (d) CIS security components preparation;
    (e) CIS security operation and maintenance (O&M);
    (f) CIS security monitoring;
    (g) SecOPs maintenance.

II.2 SecOPs executive summary

13. The executive summary summarises the necessary elements so that management can be confident that the organisation security process has been fully performed and that the results mentioned in the SecOPs integrate the concerns of the stakeholders. It has to be understandable for individuals with limited technical and security knowledge.

14. The executive summary must at least provide information on:

    (a) the SecOPs scope;
    (b) the CIS security sustainment statement.

SECOPS SCOPE

15. The executive summary must present the essential aspects of the CIS purpose and scope. The security objectives defined for the system must be summarised as in the Table 1.

	C	I	A
Business information content	**Level met**		**Partially met**
Business information exchange		**Level met**	
CIS		**Partially met**	

Table 1 - Example of Business and System security objectives

CIS SECURITY SUSTAINMENT STATEMENT

16. The executive summary must be signed by the SAA, the IAOA, IT and resources management and business owners to confirm that the system security can be sustained in accordance with this SecOPs.

17. The executive summary must also mention if all stakeholders can concur with the conclusions of the SecOPs or not, in which case the discrepancies must be detailed.

II.3 SecOPs scope

18. The SecOPs have an introduction stating the scope of the document and clearly identifying those stakeholders involved in the CIS security.

19. The SecOPs must describe the CIS in general terms either by referring to the appropriate paragraphs of the SSRS, particularly its CIS purpose and scope section, or by including this information in an annex to the SecOPs.

20. The scope must at least include information on:

(a) the CIS security requirements coverage;
(b) the CIS security environments;
(c) the persons responsible for CIS security.

CIS SECURITY REQUIREMENTS COVERAGE

21. This must describe to what extent the security requirements defined in the SSRS of the system are appropriately covered by the components implemented in the CIS (see Table 1).

CIS SECURITY ENVIRONMENTS

22. The SecOPs must precisely define security environments to demarcate the security responsibilities in a CIS. Security environments usually fall into one of the following:

    (a) the Electronic Security Environment (ESE) which is the CIS itself;
    (b) the Local Security Environment (LSE) which is the security environment within the realm of the CIS IAOA;
    (c) the General Security Environment (GSE) which is the general physical security environment in which the CIS is located. The GSE may comprise a number of disjointed general environments.

PERSONS RESPONSIBLE FOR CIS SECURITY

23. The SecOPs must exhaustively define the various roles (business user, administrator, procurement, auditor…) linked to the system. Roles related to security activities must be linked to training requirements (academic degree, certification…) as a key indicator of risk.

24. Every person in charge of security activities must be authenticated individually. When a team is in charge of a specific security activity outside the boundary of the system, appropriate mechanisms of identification and authentication must be put in place to be able to trace actions back to the author.

25. Every role will be described in a "Terms of Reference" (ToR), to be dated and signed by the persons in charge. All ToR will at least include:

    (a) the sphere of competence in terms of security environment(s) boundaries;
    (b) the duties and responsibilities of the role;
    (c) the positive descriptions of the authorised actions, by preference linked to processes in place;
    (d) the subordination within the security hierarchy.

    ToR may never authorise that a role is its own and single security auditor.

II.4 CIS security components

COMPONENTS SELECTION

26. The SecOPs must mention:

    (a) whether or not the selected security components are included in lists of approved or recommended security components (e.g. Enterprise Security Architecture). If not this choice must be justified and available experience and skills in support of this component must be detailed;
    (b) the rationale to select a specific component when several ones are available to fulfil the same security requirement;
    (c) the rationale behind the choice of making a component either active or dormant.

    Where appropriate, justifications can be detailed in a specific document.

27. The SecOPs must contain a mapping table between the security requirements stated in the SSRS and the security components chosen for the implementation. The table must also mention for each component:

    (a) the measurable key indicator(s) whose value and evolution will help in assessing its vulnerability posture;
    (b) the security environment, with its primary security responsible, where the component is used.

COMPONENTS DETAILS DESCRIPTION

28. The following types of components should be considered: personnel, facilities, media, hardware, software, communications, information and system as a whole when the description is generic.

29. The SecOPs must describe the components from three viewpoints:

    (a) preparation activities to be performed on these components (through tailored configuration and installation) before their actual use in the system;
    (b) O&M activities to be performed when these components are part of the CIS;
    (c) monitoring activities to be performed on the system.

30. When available resources allow the assignment of these activities to different teams, a separate detailed annex should be drawn up for preparation activities (e.g. see Annex 2), O&M activities (e.g. see Annex 3) and monitoring activities (e.g. see Annex 4). These detailed annexes should be summarised in a table (e.g. see Annex 1) to provide an overview of the different contents.

31. Each annex may include a separate page (e.g. Annex X – App yy) for each component to be detailed. Where appropriate the page should include the relevant system security view(s) the component is contributing to.

32. The O&M annex must detail on separate pages the security aspects that are relevant for at least the following two roles:

    (a) privileged users, clearly defining authorised actions and responsibilities;
    (b) business users. This page ("User SecOPs") should be concise and be drafted in clear, plain language, understandable by any business users. It should only address those aspects which are of importance to use the CIS correctly from a business user viewpoint.

33. The SecOPs must also define if other processes outside the scope of the CIS must also be put in place to support the system security (e.g. procurement chain…), in which case the details will be provided on how to make it conform to the security objectives (e.g. service level agreement…).

II.5 CIS security components preparation

34. The SecOPs must detail the security attributes to be presented by the components of the system. The preparation annex must at least mention:

    (a) the native attributes to be requested when developing or procuring these components (e.g. an academic degree for a technician, a TEMPEST capability for a server…);
    (b) the attributes to be added (e.g. the initial security briefing for a user, the security configuration for an operating system, the specific installation criteria for wires…), with the supporting processes to implement and maintain them up to date;
    (c) a description of the configuration and installation requirements.

35. The components will be tailored according to the configurations developed during the engineering phase of the system. The SecOPs must define how those prepared components will be assessed for conformity before the components may be part of the system (e.g. use of a test environment…), and how conformity will be regularly tested when the components are part of the system.

36. When in use in the CIS, further modifications of the components will be controlled through a configuration management process performed by the O&M actors.

II.6 CIS security operation and maintenance

37. The SecOPs must include detailed processes on how to operate and maintain the system in its security posture as defined in the accreditation decision. The SecOPs must at least address in detail the configuration and access management aspects of the CIS.

CONFIGURATION MANAGEMENT

38. A configuration management process will be defined to identify, control, account for and audit all security related changes made during the O&M of the CIS. The original configuration will be taken from the accredited configuration baseline resulting from the engineering phase of the system.

39. The SecOPs must detail the processes in place to keep up to date a Configuration Management Database (CMDB) and to control at regular intervals:

    (a) the CMDB integrity;
    (b) the conformity of the system against the CMDB data.

ACCESS MANAGEMENT

40. The SecOPs must detail the processes in place to ensure that the access controls and the privilege granted to entities (i.e. business user, system administrator, CIS internal process…) are precisely defined, controlled and audited.

SECURITY MANAGEMENT

41. In addition, the SecOPs must detail the operational processes in place to ensure that the security of the system is continuously controlled and aligned on the security posture as defined in the accreditation decision.

42. The SecOPs must at least[3] include the management details of the following aspects: security resources allocation, malware protection, backup and archiving. The operation continuity aspect must also be described, with a clear delineation between the activities to be performed by the O&M actors (e.g. for urgent reaction) and those to be performed as part of the contingency plans controlled by the monitoring team.

II.7 CIS security monitoring

43. The SecOPs should detail the specific measures in place to detect and react to unexpected actions on the system. These measures should be devoted to a specific team in order to separate the security responsibilities between the O&M actors and those in charge of the system security monitoring.

44. The SecOPs must detail at least the following aspects:

(a) CIS activity audit;
(b) CIS risk and security postures assessment;
(c) CIS emergency and contingency plans.

CIS ACTIVITY AUDIT

45. The SecOPs must detail the arrangements:

(a) to audit the activities performed by the preparation and O&M actors;
(b) to inspect / review at regular intervals the effectiveness of the security controls.

CIS RISK AND SECURITY POSTURES ASSESSMENT

46. The SecOPs must detail how risk and security postures will be assessed on a continuous basis. The SecOPs have to mention how these assessments are made (e.g. key indicators monitoring) and must detail the processes leading to a revision of the system accreditation or of the implemented security controls.

47. These assessments will be linked to dormant controls, the circumstances for their activations (e.g. key indicators of early-warning signs…) with activation details included in the contingency plans.

[3] The SecOPs may refer to the relevant controls or processes defined in the IASG 1-02 (SSRS guidelines).

CIS EMERGENCY AND CONTINGENCY PLANS

48. The SecOPs must detail responses to unauthorised or unexpected events, detailing the controls to be activated when needed. The SecOPs must also define priorities when different levels and natures of impacts (e.g. human casualties, power failure…) can simultaneously result from these events.

49. The SecOPs must describe the exercising of emergency and contingency procedures and the frequency with which exercises take place.

II.8 SecOPs maintenance

50. Following accreditation, the SecOPs must be maintained under rigorous control.

51. The SecOPs may only be changed after agreement by both the IAOA and the SAA who will define the facts potentially leading to a revision of the SecOPs in coordination with the other stakeholders.

52. The minimum facts to consider are:

    (a) changes to the risk posture;
    (b) changes to the security requirements;
    (c) changes in key indicators leading to a significant impact on trust to be placed in security measures;
    (d) changes in the system resources impacting the implemented security measures.

Annex 1

CIS SECURITY SUSTAINMENT ACTIVITIES SUMMARY

The following activities are detailed in the indicated annexes. Each domain can be divided to address specific concerns (e.g: software as O.S, bureautic…, personnel as administrator, business user…).

	Attributes		**Processes**		
	Expected attribute(s)	**Attribute(s) to be added**	**Preparation (Annex 2)**	**O&M (Annex 3)**	**Monitoring (Annex 4)**
Personnel (common)	Clearance level X	EU Sec rules briefing		Request for access Privilege management	User Error auditing Wrong activities follow-up
Administrator	IT degree Clearance level X+1				
Business user		Use of system software	User training	User responsibility briefing	
Physical	Wall resistance			Visits and logbook…	
Media			Testing process Marking process	Inventory process (CM process #xx) Data erasing process	
Hardware	TEMPEST xxx	Security seals			
Software					
O.S.		EU configuration #xx			
bureautic				CMDB process #yy	
Communication					
Information		Categorisation		Classification	
System				CMDB	Data leakage process

Annex 2

CIS SECURITY PREPARATION ANNEX

I. List of annexes

1. The following annexes will be provided:
   a) list of current security preparation responsibles;
   b) list of components details preparation;
   c) …

II. Annexes

1. List of current security preparation responsibles.
   This list will mention the individuals' name with their assigned roles and ToR. On every change and at least every six months, this list will be updated, signed and dated by the IAOA.
2. List of components.
   a) Each component (or type of components) should be described in terms of configuration and installation requirements, refering by preference to accepted standards.
   b) Particular settings of components should be put in separate appendixes when more appropriate.
3. …

III. Templates

1. Certificate of configuration conformance.
2. Report of installation inspection.

Annex 3

CIS SECURITY OPERATION AND MAINTENANCE ANNEX

I List of annexes

1. The following annexes will be provided:
   a) list of current security O&M responsibles;
   b) list of autorised O&M activities and actions;
   c)…

II. Annexes

1. List of current security O&M responsibles.
   This list will mention the individuals' name with their assigned roles and ToR. On every change and at least every six months, this list will be updated, signed and dated by the IAOA.
2. …

III. Templates

1. User responsibility briefing.
2. Change request.
3. Logbook to access protected rooms;
4. …

Annex 4

CIS SECURITY MONITORING ANNEX

I List of annexes

1. The following annexes will be provided:
   a) list of current security monitoring responsibles;
   b) list of minimum monitored events;
   c) list of dormant controls and activation conditions;
   d) list of contingency activities;
   e) …

II Annexes

1. List of current security monitoring responsibles.

   This list will mention the individuals' name with their assigned roles and ToR. On every change and at least every six months, this list will be updated, signed and dated by the IAOA.

2. …

III Templates

1. Incident report.

2. …