COUNCIL OF THE EUROPEAN UNION

Brussels, 14 November 2013

16085/13

CSCI 61
CSC 142

NOTE

From :	The General Secretariat
To :	Delegations
Subject :	Information Assurance Security Guidelines on System-specific Security Requirement Statement (SSRS)

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 System-specific Security Requirement Statement (SSRS) on the 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 System-specific Security Requirement Statement (SSRS)

IASG 1-02

This version replaces ISP 201 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 structure and the content of the System-specific Security Requirement Statement (SSRS) which has to be developed for each Communication and Information System (CIS) handling EUCI.

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

4. 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 CSR mandate the development of CIS security documentation, in particular the SSRS which is 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 an SSRS which defines how the system fulfils the requirements laid down in the CSR and underlying security policies and guidelines. The SSRS must be communicated to the system stakeholders.

8. As stated in the IASP L[2], the development of the SSRS is started when a CIS project is initiated and is progressively enhanced based on the outcomes of the justification and engineering phases of the CIS life cycle.

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

9. The SSRS documents what it means for a specific system to be appropriately secure in the particular context in which it will be used. This is done through a reasoned, risk-based elicitation of security requirements, specified at the security service level. Each security requirement mandates minimum acceptable levels of strength and assurance to be met by potential mechanisms and products used for its implementation.

10. The SSRS consequently forms the basis for the formulation of Security Operating Procedures (SecOPs) which explain in detail the actual security implementation in the final system.

11. The SSRS is therefore a governance document of the system security posture, stating all the security requirements to be implemented when considering the full potential risk posture of the system.

12. Dynamic assessment of this risk posture through relevant key indicators on risk components will lead to partial or full activation of these requirements in order to remain within acceptable limits of protection.

13. When approved by the SAA, the SSRS forms a binding agreement between the IAOA and the CIS stakeholders on the security requirements.

14. In principle the SSRS is classified R-UE/UE-R. When some elements included in the SSRS 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 SSRS.

II. SYSTEM-SPECIFIC SECURITY REQUIREMENT STATEMENT

II.1 SSRS layout

15. The SSRS is composed of different sections organised as follows:

    (a) SSRS executive summary;
    (b) SSRS scope;
    (c) CIS security objectives;
    (d) CIS risk statement;
    (e) CIS security requirements;
    (f) SSRS maintenance.

II.2 SSRS executive summary

16. This section must at least provide summary information on:

    (a) the SSRS scope;

    (b) the residual risk statement; and

    (c) a generic overview of the security requirements categories;

    and any other necessary elements so that management can be confident that system security is in line with the business needs and the organisational security strategy. It has to be understandable for individuals with limited technical and security knowledge.

17. Drafted at the end of the engineering phase, it confirms that the organisation security process has been fully performed and that the results set out in the SSRS integrate the concerns of stakeholders.

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

19. The executive summary must be signed by the main stakeholders (the SAA, the IAOA, IT and resources management and business owners).

SSRS SCOPE

20. The executive summary must present the essential aspects of the CIS purpose and scope, its description and stakeholders and the security solution.

21. The security objectives defined for the system must be summarised as the example in Table 1 (authenticity and non-repudiation may be added when relevant).

	C	**I**	**A**
Business information content	**x**		**x**
Business information exchange		**x**	
CIS		**x**	

Table 1 - Example of Business and System security objectives

CIS RESIDUAL RISK STATEMENT

22. This section states the general view of the expected risk posture after implementation of the permanent security requirements, mentioning the events potentially leading to the activation of additional security requirements.

23. The most important residual risks must be presented in terms of business impacts (e.g. business assets' initial and end states, associated by a threat event).

CIS SECURITY REQUIREMENTS SUMMARY

24. The summary must refer to the agreed list of organisational potential security requirements, mentioning those having been retained for implementation, for example:

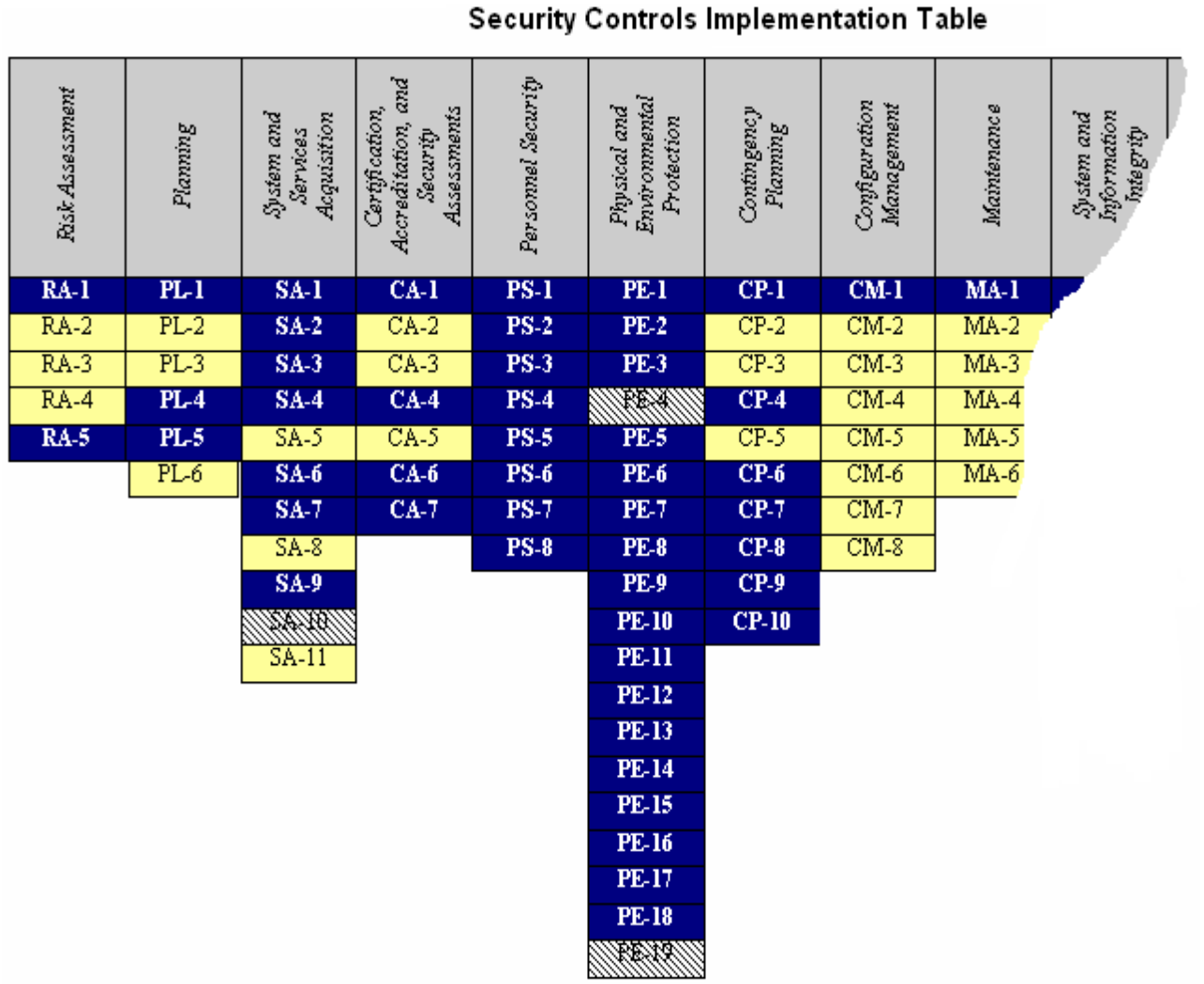

Figure 1 – Extract from NIST SP 800-53, as example at this stage - To be replaced by ISM³ (Information Security Management Maturity Model) if accepted

II.3 SSRS scope

25. The introduction to the SSRS states the document's scope, the basic facts about the system and identifies those involved in its security. This information is the baseline for establishing the security requirements and also a point of reference for the future.

26. The SSRS must at least provide information on:

    (a) the CIS purpose and scope;
    (b) the applicable context in which the CIS will operate;
    (c) the system stakeholders;
    (d) the information flows to be protected by the CIS.

CIS PURPOSE AND SCOPE

27. An accurate SSRS depends on a clear and precise definition of the purpose and scope of the system to be secured. There must be a concise unequivocal definition of the system, referring, where appropriate, to CIS project management and accreditation documents sets instead of duplicating their content. Useful aspects to be mentioned are:

    (a) the basic CIS references (name, purpose, strategic importance, User Security Operationl Requirements (USOR)…);
    (b) the main assets with their relevant security attributes;
    (c) the expected behaviours in terms of information flows and authorised workarounds;
    (d) the actors in contact with the system;
    (e) the place and conditions of use.

28. An essential element of information flows is the definition of system interfaces, not only with the users but also with other systems, especially those considered for potential interconnections.

APPLICABLE CONTEXT

29. The SSRS must describe contextual aspects which could have an impact on the future solution. Potential contextual aspects to be considered are the organisational culture and strategy, resources, security rules and policies, IT and security master plans, key business drivers, potential impact on stakeholders and partners, etc.

30. These aspects can have several implications, for instances the nature of threats or the counter-measures to be chosen when implementing the security requirements.

SYSTEM STAKEHOLDERS

31. The SSRS must list system stakeholders (business, financial, IT…), especially those who can take decisions on the resources required to implement and sustain the security counter-measures.

INFORMATION FLOWS ARCHITECTURE

32. The SSRS must explain which information flows should be protected. The architecture diagram(s) must use an agreed modelling method allowing business stakeholders to verify that their processes are adequately understood and represented.

33. In modelling the processes, preference should be given to business modelling standards which allow a formalised representation of the security concerns and which can be easily re-used in the CIS development (e.g. Unified Modelling Language (UML) use-cases and diagrams).

34. The SSRS could refer to essential use cases, or similar representations, to analyse business process courses of action and authorised states, with the aim of identifying potential checkpoints for security supporting services.

II.4 CIS security objectives

35. This section is aimed at stakeholders concerned by the security objectives and the implemented solution but not necessarily interested in all aspects of risk assessment and security requirements elicitation.

36. Based on the business needs and context, the IAOA must identify the expected protection objectives which should be enforced in the final system. The identification of these objectives is expressed in high level, technology-independent, statements of what the system security should be able to do.

37. The objectives must be measurable, achievable and realistic and should be best expressed as positive statements formally stating what the system is authorised to do.

38. The objectives must be ranked by importance to be used as rationales when having to justify the implementation and expenses of security requirements.

39. The IAOA must mention how these objectives have been elicited (referring to an agreed list of security objectives, brainstorming sessions, specific techniques….) to allow the stakeholders to be convinced of the completeness of the elicited objectives.

40. The SSRS must distinguish between the security objectives supporting native business needs from those derived from contextual aspects the final system has to comply with.

41. The SSRS must at least provide information on:

    (a) the business based security objectives and their rationale;
    (b) the context based security objectives and their rationale;
    (c) the "To-Be" system security architecture.

BUSINESS BASED SECURITY OBJECTIVES

42. Based on the information flows defined within the scope, the SSRS must explicitly elicit the business security objectives supporting the system in meeting the business needs as identified in phase 1 of the CIS life cycle[3].

43. The business security objectives have to be formally linked to business impacts in case of loss of confidentiality, integrity and/or availability (and where appropriate authenticity and non-repudiation) for the different business assets being considered. This impacts assessment can then be used as a security key indicator for the importance of a security breach.

CONTEXT BASED SECURITY OBJECTIVES

44. The native business security objectives are only one aspect of creating a secure system. The CIS *per se* must also fulfil security objectives generated by the specific contextual aspects (legal requirements, organisational strategy, IT and security master plans, place of use…) the CIS has to comply with.

45. Each contextual aspect must be carefully assessed, to detect additional needs imposed by these legal or regulatory obligations (e.g. protection of privacy…), organisation strategy (e.g. Enterprise Architecture…) etc., and elicit the relevant security objectives.

CIS SECURITY ARCHITECTURE

46. The SSRS must present the security architecture which has been chosen as an acceptable solution for the security objectives to be fulfilled. This architecture constitutes the “To-Be” for the final system.

[3] See Doc 16268/12 - IASP L

47. This architecture will be available for inclusion in the SSRS after the relevant stakeholders have performed a trade-off analysis between the potential designs and solutions meeting the security requirements listed later in the SSRS.

48. The size of the architecture could require the definition of several views and their relationships, in which case the IAOA and the SAA can decide to address each view independently. In this case the IAOA must provide a general overview of the system and details by views should be described in annexes. However the IAOA must always avoid an architecture whose complexity could constitute *per se* a security vulnerability.

49. A graphical approach could be best suited to provide a compact overview of the complete security picture instead of an extensive amount of text. This representation will lay stress on security functionalities reducing risks instead of system components details.

50. The SSRS must mention the resources to be made available for implementing this architecture and a traceability matrix, mapping business and context needs to security objectives and solutions, has to be provided.

II.5 CIS risk statement

51. The full risk assessment (RA) exercise is not part of the SSRS, but the stakeholders must be able to find in this section the relevant information to be able to satisfy themselves that the RA recommendations can be trusted.

52. The SSRS must document how it has been dealt with the uncertainty behind risk assessment components (such as likelihood or completeness of landscapes (threats, vulnerabilities)) and therefore to which extent the risk assessment outcomes give an accurate representation of the system risk posture. The stakeholders have to understand how the risks have been identified, which metric is used to consider a risk as acceptable and how the requirements are selected to truly mitigate the risks.

53. The SSRS must also document how some RA values (such as likelihood estimates, absence or presence of vulnerability, threat agent presence…) are characterised by key indicators which will be used as inputs for a dynamic assessment of the risk posture and the activation of appropriate security requirements in order, for the system security, to remain within agreed limits during the whole CIS life cycle.

54. The SSRS must at least provide information on:

(a) the RA components;

(b) the risk acceptance criteria;

(c) the residual risk posture.

RISK ASSESSMENT COMPONENTS

55. A security risk assessment can only be deemed accurate if stakeholders can trust the estimates made on its components (threats with their attributes, vulnerabilities, system impacts, business impacts…) in terms of value or completeness. The trust to be placed in these estimates will provide appropriate justifications for actions and expenses.

56. The following information must be provided:

(a) the databases considered as relevant and complete for the RA components;

(b) the rationales (statistics, expert judgement…) used to estimate the values linked to these RA components (likelihood of a threat, threat actor strength, likelihood of weaknesses…);

(c) the risk modelling technique (scenario, attack trees, abuse cases…) and its relevance to actually represent the risk landscape;

(d) the rationales used to assess the value of impacts should a risk become effective;

(e) the metrics used to define the required levels of strength and assurance to be presented by the security mechanisms and products to appropriately decrease the risks.

57. This information must be supported by measurable key indicators whose values and evolutions will help to assess if the actual system security posture remains in line with the current risk posture.

RISK ACCEPTANCE CRITERIA

58. The SSRS must define against what the risks have been assessed. It is recommended to use a risk matrix representation which allows some kind of flexibility for what must be implemented, depending on the variation of the value of the RA components.

59. One way to do this is using a risk appetite matrix, e.g.

		Business Impact				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare				Risk 03	
	Unlikely	Risk 01				
	Possible		Risk 02			
	Likely				Risk 04	
	Certain					
		Acceptable	To-be-discussed		Unacceptable	

Table 2 - Eexample of risk appetite matrix

60. Risk estimates always include a factor of uncertainty. Estimates of likelihood, potential impacts, quality of counter-measures, etc. can only be estimated within limits. This variation in likelihood and impacts lead to “To-be-discussed” zones of risks to be taken into account based on the value of the key indicators.

61. The SSRS must also refer to the organisational risk preference for prioritisation during the risk treatment phase when it is not possible to protect all the different types of impacts (image, business course of events…) with the available resources.

RESIDUAL RISK POSTURE

62. It is recommended to present two system risk postures:

(a) initial, assuming no security requirement is implemented;

(b) targeted, made of the residual risks, assuming all the recommended security requirements (immediate and delayed) are in place to ensure that all risks are considered and will be subsequently monitored.

63. The SSRS must mention the maximum and minimum risk postures for the system when the security requirements are partially or totally active.

II.6 CIS security requirements

64. This section specifies how security is to be implemented, sustained and monitored. The security requirements describe what has to be done to reduce the likelihood and impact of the identified risk to accepted levels.

65. The security requirements must be linked to risks and security objectives to ensure that the list of security requirements is consistent and complete.

66. The security requirements must be high-level statements, mandating a minimum level of strength and assurance for the mechanisms and products used to counter a specific risk. These strength and assurance values provide security engineering guidance but allow alternatives solutions.

67. The compliant mechanisms and products must be taken from the Enterprise Security Architecture (ESA), as defined in the IASP L, as it constitutes a reference of mechanisms and products whose content and implementation are correctly mastered.

68. The list of requirements must be defined per asset following the SecOPs layout. There must be a prioritisation framework of the security requirements, based on the relevant business needs that are supported by the CIS.

69. The SSRS must at least provide information on:

    (a) the requirements selection process;
    (b) the selected requirements for initial implementation and decision rationale;
    (c) the selected requirements for activation on request and conditional circumstances for this activation.

REQUIREMENTS SELECTION

70. The SSRS must set out the rationales behind the choices of requirements.

71. The security requirements may be extracted from agreed lists to help in formally and unambiguously expressing them. New security requirements may be added when no available security requirement meets the expected requirement aim.

72. These lists of potential security requirements should aim at reaching an acceptable level of security maturity when taking into account the available resources in place instead of trying to enforce strict compliance to specific standards which do not often weight the importance of security controls against each other.

73. The organisation must define a protection strategy to decide between immediate or delayed enforcement of security requirements:

    (a) the first ones are part of the original setup of the system and activated;
    (b) the others are prepared but only activated when needed.

74. This delineation combined with the risk components key indicators will support the enforcement of a dynamic security posture where:

    (a) the security requirements stated in the SSRS address all the relevant potential risks;
    (b) the actual security mechanisms and products detailed in the SecOPs can be activated as required by the current risk posture to ensure that the system security posture remains within the authorised limits.

75. This delineation will allow to not only know how the system is protected but more importantly against what it has been decided to not protect it immediately.

REQUIREMENTS TO BE IMPLEMENTED

76. This paragraph identifies the security requirements that have been derived from the risk assessment and are considered relevant for direct implementation.

77. The SSRS has also to mention if some criteria must be used for the selection of further mechanisms and products (economic principles, compliance, rating approach…) when implementing these requirements.

REQUIREMENTS TO BE ACTIVATED ON REQUEST

78. This paragraph identifies the security requirements that have been derived from the risk assessment and considered relevant but will not be activated due to specific considerations (e.g. lack of resources…). Examples are:

    (a) security requirements against a cyber attack that could not be supported by accurate likelihood estimates;
    (b) security mechanisms which could be counter-productive for the organisation if activated on a large scale (e.g. blocking network segments to avoid malware dissemination).

79. These security requirements should be prepared but not activated until sufficient early-warning signs (important zero-day flaw, increase in network reconnaissance activities…) can be used as key indicators to justify the activation of dormant counter-measures. The activation of these security requirements must be detailed in the necessary contingency plans.

II.7 SSRS maintenance

80. Following accreditation, the SSRS must be maintained under rigorous configuration control.

81. The SSRS 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 SSRS in coordination with the other stakeholders.

82. The minimum facts to consider are:

(a) changes of the security objectives;

(b) changes of the context as defined in the IASP L;

(c) changes in key indicators leading to a significant influence on the results of the RA and the security requirements;

(d) changes in the system resources impacting the implemented counter-measures.