WHAT ARE SECURITY DOCUMENTS FOR?

- Objectives of MOD's Accreditation Documents

Clare Robinson and Kay Hughes
clrobinson@QinetiQ.com and kjhughes1@QinetiQ.com
WWB006, QinetiQ, St Andrew's Road, Malvern, Worcs. WR14 3PS

Abstract

Domain Based Security concepts have helped to define the new MOD approach to security policy documents. This paper introduces the MOD security documents that support the issue of an accreditation certificate and subsequent maintenance of accredited status. It relates them to the documentation approaches in HMG Infosec Standard Number 2 and CESG Memo 5, and also to the IS017799/BS7799 information security management standard.

Keywords

Accreditation, security documents, Domain Based Security, IS2 Accreditation Document Set, System Security Policy

1 Introduction

1.1. MOD policy is that any MOD Communications and Information System (CIS) that will store, process or forward any official information should be accredited before use. Accreditation decisions are made on the basis of evidence of adequate security risk management. The objective is to demonstrate that all relevant security risks to the CIS have been identified and will be appropriately managed by its intended configuration, use, maintenance, evolution and eventual disposal.

1.2. In such a diverse department as MOD, a single approach to accreditation evidence would not be appropriate. Hence, MOD permits different kinds of accreditation evidence to support different kinds of system and projects. MOD's accreditation requirements fall into two broad categories:

a. Registration and compliance with generic documentation for simple systems. This case is considered no further in this paper;

b. Registration with the accreditor at the start of a project, followed by the production of project-specific security documents in support of the issue of an accreditation certificate.

1.3. The accreditor's decision must be based on a clearly defined security case provided by the project. The project should justify to the accreditor that the security constraints and controls they are providing are sufficient to satisfy MOD policy. Although accreditors can have an important advisory/guiding role, the onus should be on a project to submit their security case for a project-independent security risk management check.

1.4. However, security documents to support the on-going process of operational security risk management and compliance checking are at least as important as those which present the initial case for accreditation. It is the actions of the people who use and manage a CIS that ultimately determine whether or not it is secure, not the accreditor. Hence, accreditation documents should support an on-going process, and not be aimed at a one-off accreditation event.

1.5. MOD security documents are intended to be short, well-focussed and useful. The objective of any document should be clear to those who produce it and those who are asked to authorise and use it. Security-relevant information may be intended to:

a. Instruct and inform the people who use and manage a CIS as part of their day-to-day operational view of security;

b. Provide evidence to support an accreditation decision, as part of the accreditors' and compliance checkers' view of security;

c. Support and inform the change management process;

d. Manage security-related project risk arising from the impact of the need for security controls and accreditation on the procurement process.

1.6. This paper discusses the operational, change and accreditation views of the security of a CIS, and the security documents that provide them. These documents comprise the MOD Accreditation Document Set. The paper relates these MOD documents to an Infosec Standard Number 2 Accreditation Document Set (ADS) [2] and a traditional CESG Memo 5 System Security Policy (SSP) [6]. Finally, the paper considers the relationship between the MOD documents and the IS017799/BS7799[7] information security management standard. The paper concludes with some observations.

1.7. MOD's approach to product risk reduction is focussed on agreeing an accreditation strategy, and detailed discussion is outside the scope of this paper. For further information see Defence Information Assurance Notice (DIAN) number 7 [1], or the overview in the paper [5].

1.8. Details of the MOD document structures and how to produce them are also outside the scope of this paper. Instead, DIAN/07 [1] should be consulted.

2 Overview of the MOD accreditation documents

Roadmap

2.1. Figure 1 illustrates the three views of the security of an accredited CIS and identifies the security documents that comprise them. The key document for each view is shaded grey. Overviews of each of the security documents are given below Figure 1 and in the remainder of this paper.

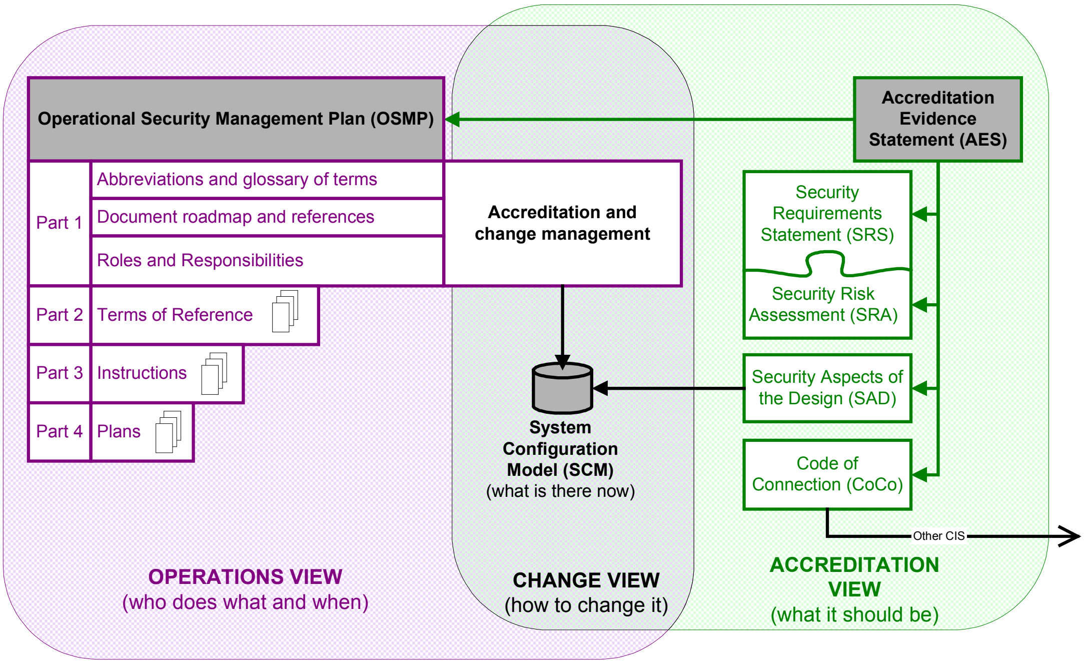
Operational Security Management Plan (OSMP)
Accreditation Evidence Statement (AES)
Part 1
Abbreviations and glossary of terms
Document roadmap and references
Roles and Responsibilities
Accreditation and change management
Part 2
Terms of Reference
Part 3
Instructions
Part 4
Plans
Security Requirements Statement (SRS)
Security Risk Assessment (SRA)
Security Aspects of the Design (SAD)
Code of Connection (CoCo)
System Configuration Model (SCM)
(what is there now)
Other CIS
OPERATIONS VIEW
(who does what and when)
CHANGE VIEW
(how to change it)
ACCREDITATION VIEW
(what it should be)

Figure 1: roadmap to the accreditation documents

2.2. On the left of Figure 1, the 'operations view' defines who should do what and when, to ensure that the CIS is used and managed securely. The focus of this view is the Operational Security Management Plan (OSMP).

2.3. On the right of Figure 1, the 'accreditation view' lists all the documents and activities (such as inspections) that support the issue of the accreditation certificate. The focus of this view is the Accreditation Evidence Statement (AES). The other documents provide descriptions of the security relevant properties of the CIS, including the risk assessment, requirements and design information, and include the OSMP.

2.4. The ‘change view’ links the accreditation and operations views. It is centred on the current configuration of the CIS, defined by the System Configuration Model (SCM), and the OSMP policies and procedures for accreditation and change management. Decisions on change management may need to refer to any or all of the other project-related documents, or to outside policy documents.

2.5. The security requirements and risk assessment are closely linked, in that one cannot be agreed without the other. Hence, in Figure 1 they are depicted as two halves of a jigsaw. Although the other security documents are also dependent upon each other, they are not so tightly coupled, and may be produced and authorised more independently.

Relationship to other documentation approaches

2.6. Traditionally, security has been documented as a System Security Policy (SSP) and Security Operating Procedures (SyOPs). Essentially, the SSP provided the accreditor’s view of security and how it was implemented. The SyOPs were the users view. Both SSPs and SyOPs could be cumbersome documents and were not always amenable to change as the system was maintained and evolved. The new MOD approach is focussed on the need for short, useful security documents that support accreditation and change management for a CIS, as well as securing day-to-day operation as first envisaged.

2.7. Within HMG, the concept of an Infosec Standard Number 2 Accreditation Document Set (IS2 ADS) [2] has replaced the concept of an SSP and SyOPs. An Operational Security Management Plan (OSMP), supported by the other documents, is effectively an alternative structuring of the contents of an IS2 ADS. To avoid confusion it has been given a different name. However, there is an important difference in emphasis between an IS2 ADS and an OSMP. An IS2 ADS is focussed on providing the accreditors with the information they need to accredit a system, supported by the SyOPs for the users. The OSMP, however, is focussed on providing the information needed to use, manage and maintain the system securely. Although the needs of the accreditors are important, they are not the primary driver for the structure of the new MOD security documents.

2.8. Note that the approach defined by MOD includes the process of producing and agreeing security documents. Although IS2 recognises the need for such a process, it does not define how it should be conducted or the security documents to support it. In the majority of projects, the request for accreditation will not be the first involvement of the accreditor in a project. Normally, accreditation is expected to be granted on the basis of a previously agreed risk management approach and supporting security documents. Hence, the focus of accreditation documents on operational needs, rather than the accreditor is entirely appropriate.

2.9. IS2 provides a framework for documentation to support the accreditation across government. It emphasises local departmental autonomy and encourages departments to adapt the standard for its own use. Hence, in extending the security documentation to cover the procurement process and focussing on operational needs, MOD is consistent with the intentions of IS2, if not with its proposed ADS format and structure.

3 The key MOD security documents

Accreditation Evidence Statement (AES)

3.1. The AES concept provides the flexibility for the wide range of MOD projects to agree the project-specific pre-requisites for accreditation. An AES lists the security documents and activities which support the accreditation of a CIS, some of which may be the responsibility of third parties. Ideally, it should be provided as a checklist on a single side of A4. An AES can support both procurement and post-accreditation security activities.

3.2. Procurement: By producing and agreeing an AES for every accreditation decision, including any interim accreditations, a project minimises the risk that unplanned documents or activities to support accreditation will be required. The AES includes a description of the Target of Accreditation, together with target dates and a traffic light system to gauge progress towards the accreditation milestones. OSMP-based accreditation evidence is recommended, although other approaches are permitted. For example, legacy documentation may be upgraded where a complete overhaul of the security documentation would not be cost-effective.

3.3. Post accreditation: By attaching an AES to the accreditation certificate, it can be used as the top level security document for the accreditors and compliance checkers. It acts as a 'contents list' for the set of accreditation documents, including inspection reports. The target dates can be used to record the dates for compliance checking reviews and inspections. By listing all the components of accreditation evidence, the AES can also help with the application of the change management policy, see section 4.

3.4. The use of an AES as a 'contents list' is consistent with the guidance in IS2 [2], although broader in scope. Unlike the contents list of an IS2 ADS, an AES also provides a checklist for the non-documentary activities that support accreditation within MOD, such as site inspections.

3.5. By making the short Accreditation Evidence Statement (AES) the top level view for the accreditors and compliance checkers, the emphasis for the more detailed accreditation evidence documents has been placed on supporting security management in service. Hence, the name Operational Security Management Plan (OSMP) for the top level document for the people who use, manage and maintain a CIS.

Operational Security Management Plan (OSMP)

3.6. The purpose of an OSMP is to communicate how a CIS is to be securely configured, used, managed, maintained, upgraded and disposed of to the people who are responsible for doing so. An OSMP is intended to provide security relevant information in a clear, concise and usable form. Hence, the accreditors may have confidence that the security instructions and procedures will be followed. By demonstrating that an appropriate security management regime has been defined, an OSMP can also provide evidence to support the accreditation of a CIS.

3.7. The OSMP is the top level of the security portfolio for these people, and should clearly define the security roles and responsibilities which are being signed up to. Authorisation of the document should be a commitment to provide sufficient priority, authority and resources to these roles to enable information security management for the CIS to be carried out effectively and in accordance with the plan.

3.8. The OSMP provides the day-to-day user and management view of the system. In the same way as an IS2 ADS, it includes the documents providing the Security Operating Procedures (SyOPs). The MOD approach to SyOPs is to move towards clear and concise leaflets for specific user groups and situations, rather then monolithic documents. Hence, an OSMP explicitly structures the SyOPs as individual terms of reference, instruction leaflets, procedures and plans.

3.9. Other key components of an OSMP are:

a. A roadmap to all security documents in the portfolio. The roadmap summarises the purpose of each security document, how they relate to each other, who the document applies to, when it applies and where it is located;

b. The accreditation management policy. This defines the timescales, frequency and content of audit, inspections, compliance checking and reviews. These ensure that the OSMP is being followed and the assumptions about the operational context and dependencies remain valid.

c. The change management policy. This defines how the impact of proposed changes to the system are to be assessed and the roles and responsibilities for authorising changes. An overview of how the MOD documents can be used to support the definition and application of this policy is given in section 4.

3.10. To help ensure consistency and to avoid repetition between individual documents, an OSMP may also define the abbreviations, terms and references for the complete set of security documents.

3.11. The scope of an OSMP should be defined in terms of the people/roles who use and maintain a CIS, and not be limited to project procurement boundaries. Hence, multiple projects may contribute to a single OSMP. The contributions required from the different projects may be agreed using the AES concept as part of an overall accreditation strategy for a group of related projects. In some cases, a specific project may only need to produce security instructions for the use of a new application on existing infrastructure.

3.12. This approach is consistent with IS2, in that the scope of an ADS may be wider than a project. The difference is that the process of agreeing the scope of an ADS is not part of IS2, whereas the accreditation strategy documents that agree the scope of security documents are included in the MOD approach.

System Configuration Model (SCM)

3.13. The current configuration of a CIS is defined by the SCM. This would normally be a single sheet referring to various databases, etc., under the control of the system management. These record the lists of current authorised users, the numbers and locations of workstation, software versions, etc. The SCM is both a tool for the system managers and the basis for compliance checking.

3.14. There is no direct equivalent of the SCM concept in IS2 [2]. Depending upon the level of detail provided in an IS2 ADS, an SCM may be equivalent to some of the information in the IT Resources section of Part 1. However, the intention is that the description of the current configuration may be updated independently of the rest, as discussed in the next section.

4 Accreditation and change management

4.1. No system is static, and hence a change management policy is critical in ensuring that the security risks continue to be appropriately managed. The CIS-specifc policy will need to be agreed between a project and its accreditors, but is likely to follow the principles outlined below:

a. Changes to the configuration that are clearly consistent with design constraints may be made on the authority of the system management without requiring re-accreditation. Such changes would only affect the SCM, and a record of the changes would be kept for compliance checking. Changes falling into this category could be the introduction of new users with the same security clearances and nationalities, etc., as existing users, movement of equipment within existing sites, updating the signatures of virus checkers, etc.;

b. Configuration changes that violate design constraints are more significant, and could not be made on the authority of the system management alone. Re-accreditation of the CIS would be required, and the accreditor, or forum such as a Security Working Group, would need to be involved. Re-accreditation would be based on demonstrating that the security requirements are still met and any assumptions of the risk assessment are still valid , and could involve an independent security assessment such as a Health Check or re-evaluation. Changes falling into this category could be upgrading workstation, server or firewall technology or expanding the system onto new sites with equivalent physical and personnel security;

c. Any proposed change that does not meet the security requirements is likely to require a detailed review of the risk assessment and business requirements. Significant changes to the security design or implementation may also be required. This kind of change would need to be referred to the accreditors/Security Working Group. Changes falling into this category could be the introduction of new business connections, which may introduce new ways in which existing information or services may be compromised.

4.2. The change management policy should guide those with responsibility for carrying it out. Effective change management requires that an impact assessment of the proposed change can be carried out. To support this, there should be traceability through;

a. Security risk;

b. Effect required of the countermeasures (both security functions and separation requirements);

c. Design of the countermeasures;

d. SyOPs that support the implementation of the countermeasures.

4.3. This approach also provides a logical argument to support accreditation. Traceability is best achieved by clearly distinguishing between the security requirements, in terms of effect, and the design. Unlike a traditional SSP and an IS2 ADS, the MOD approach achieves traceability by defining separate, cross-referenced, documents that can be used to record the security risks, requirements and design. The change management policy can then be stated in terms of requirements to review these documents and the authority to approve changes.

4.4. The MOD documents answer the following questions:

a. What security is needed? Recorded in the Security Requirements Statement (SRS). This gives the detailed security requirements, including any required Evaluation Assurance Levels. It should define the security characteristics of people, data and environments, and the constraints imposed on sharing information between different groups and security controls that apply. The requirements should be stated in terms of the effect they are intended to achieve, rather than the way in solution terms.

b. Why is the required security adequate? Recorded in the Security Risk Assessment (SRA). This justifies that the security requirements meet policy. It should record the agreed security risks and how they are managed. An SRA should justify that the security functions defined in the SRS provide an adequate defence. It should also explain how the assurance requirements in the SRS have been derived.

c. How is the required security achieved? Recorded in the Security Aspects of the Design (SAD). This describes how the design and implementation meet the security requirements. It should explain the properties of the design/implementation that provide the required separation, i.e. the absence of functionality, as well as how the security functions are implemented, and how any required assurance levels have been obtained.

4.5. Recording requirements, risk assessment and design information in separate documents is a fundamental difference in approach from an IS2 ADS or SSP. It directly affects the structure and presentation of the vast majority of the security-relevant information. The flexibility provided by the IS2 ADS structure means that the distinction between requirements and design is not as clear-cut. Hence, there is no simple mapping between the sections of an IS2 ADS and the SRS, SRA and SAD. Similarly, it is not a straightforward task to provide a simple mapping to the sections of an SSP.

4.6. The MOD approach of separate SRS and SAD documents also enables the security requirements for separation and controlled sharing to be agreed independently of design detail. This can support project risk reduction and provide the security specification needed to support contract negotiations. It can enable user representatives to be involved in agreeing operationally effective security controls in terms of their business functions, rather than in terms of specific security technology.

4.7. The graphical Infosec Architecture Model notation defined in [3] can be used to provide a structure for describing security requirements in an SRS. The model can also support risk analysis for the SRA, and support mutual understanding and conflict resolution between the user and security communities. An overview of the notation and its use at different stages in a procurement was given at the Sunningdale Accreditor's Conference in 2001 [4].

5 Relationship to BS7799

5.1. BS7799 [7] specifies requirements for establishing, implementing and documenting an Information Security Management System (ISMS) for the whole, or part of, an organisation. To comply with the standard, an organisation needs to be able to demonstrate that all the control objectives and controls in the standard have been met, or to justify their exclusion from that ISMS.

5.2. The BS7799 concept of an ISMS most directly relates to high level MOD policy, and the accreditation process itself. Much of BS7799 is at a higher level than the project-specific security documents that are produced to support the accreditation, use and maintenance of a specific CIS. Similarly, many of the control objectives and controls are embodied in MOD policy and the MOD security organisations, roles and responsibilities, rather than project-specific documentation. Any compliance with the standard is likely to be at an organisational level, rather than a specific CIS, although an ISMS could be defined around a single CIS.

5.3. The objective of an ISMS is to manage effectively information security within the organisation. At the level of a specific MOD CIS, the ISMS concept corresponds most closely with the OSMP. As discussed in this paper, an OSMP is intended to communicate how to configure, use, manage, maintain, upgrade and dispose of the system securely to the people who are responsible for doing so. It includes terms of reference and security instructions of individual roles. An OSMP should be signed-off by people who can ensure that the security-relevant activities and roles defined in the document are given sufficient priority, authority and resources to enable them to be carried out effectively.

5.4. The security controls in BS7799 provide a source from which to draw the required security functions in an SRS and supporting procedures defined in an OSMP. Other sources include MOD policy documents, HMG Infosec Standard Number 3 [8] and risk assessment methods such as CRAMM. However, many of the security functions derived from such sources are solution-oriented, whereas an SRS should state the required effect of the function. A detailed mapping of the objectives and controls in BS7799 to MOD policy and the information required by the MOD accreditation documents is beyond the scope of this paper.

6 Observations

6.1. The new MOD security documents have been developed in support of the following objectives:

a. Provide adequate and demonstrable security that works across procurement boundaries;

b. Maintain security in service through both normal operation and change;

c. Manage project/procurement risk arising from the need for security controls and accreditation.

6.2. This paper has concentrated on the security documents that support the issue of an accreditation certificate. The approach taken has been to focus the security documents on the maintenance of accredited status in the context of a dynamic system, rather than on an initial accreditation event. Accreditor involvement in the procurement process has been assumed, and some additional security documents, outside the scope of this paper, are defined to support this.

6.3. The key to the approach is the separation of security requirements, risk assessment, design information and procedures/instructions into separate documents. This supports impact assessment on the changes proposed to an operational system. It can also support the initial procurement process as the security requirements and risk assessment can be agreed independently of design detail. This can reduce the risk of inadequate or insufficient security controls, before committing to the development of a solution. It also permits a degree of design freedom, enabling the most cost-effective solution to be developed.

6.4. However, this approach comes at the price of increased documentation production and authorisation overheads. It also requires strict configuration control to ensure that the separate documents are consistent. Therefore, the approach may not be cost-effective for small, relatively static systems, those with minimal security concerns or transient short term systems. If demonstrating adequate security and maintaining it through change is not a primary objective, a different documentation approach may be more appropriate. Hence, the OSMP/SRS/SRA/SAD approach is not mandatory, and MOD permits agreement of other kinds of security document to support the issue of the accreditation certificate. The key to the flexibility of the approach is the requirement to agree the project-specific accreditation strategy. This should define what security documents are required, their purpose, who should produce and authorise them and when.

7 References

1. MOD, Defence Information Assurance Notice Number 7 (Security Policy Documentation), v1.0, September 01 and Annexes A and B

2. HMG, Infosec Standard Number 2 ‘Accreditation Documents’, October 2001

3. HMG, Defence Information Assurance Notice Number 8 (Domain Approach Techniques), v1.0, September 01 and Annexes A, B and C

4. QinetiQ, ‘Security Requirements Models to Support the Accreditation Process’, QinetiQ/KIS/SEB/CP011079, presented at the 2nd Annual Sunningdale Accreditor’s Conference, 10th-11th September 2001

5. QinetiQ, ‘Managing Infosec Risk in Complex Projects’, QinetiQ/KIS/TIM/CP010069, presented at the 4th Annual Systems Engineering for Defence Conference, RMCS Shrivenham, 15th-16th February 2001

6. CESG, Electronic Information Systems Security Memorandum No. 5, System Security Polcies, Issue 3.0, July 1994

7. British Standard 7799, Information security management – Part 1: Code of practice for information security management (now ISO 17799) and Part 2: Specification for information security management systems

8. HMG, Infosec Standard Number 3 ‘Connecting Business Domains’, October 2001