EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
Informatics Security

Brussels, 23/06/2011
HR.DS5/GV/ac ARES (2011) 675291
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON ACCREDITATION PROCESS FOR COMMUNICATION AND INFORMATION SYSTEMS HANDLING EU CLASSIFIED INFORMATION

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 23/06/2011

v03_07/06/2011

TABLE OF CONTENTS

1. ADOPTION PROCEDURE

This Security Standard is adopted in accordance with Article 10(3) of Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission, adopted on 16 August 2006.

It is drawn up under the responsibility of the Security Directorate pursuant to Article 9(1)(b) and takes into account the items listed in Article 10(2) of Commission Decision C(2006)3602, in particular internationally recognised norms and standards applicable in the field of information systems security.

Under Article 10(3) of Commission Decision C(2006) 3602, the implementing rules may be supplemented by measures of a technical, physical, procedural or organisational nature proposed by the Director of the Security Directorate and adopted by the Director-General of the Directorate-General for Human Resources and Security in consultation with departments that have a legitimate interest. These supplementary measures are called 'security standards' where their application is mandatory, or 'security guidelines' where their application is optional or where they provide guidance on security standards implementation.

2. INTRODUCTION

This document defines the Accreditation Process that all Communication and Information Systems (CIS) of the Commission processing EU classified information shall undergo as stipulated by Commission Decision of 16 August 2006 C(2006) 3602 concerning the security of information systems used by the European Commission ([3602]) and Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure and amendments [844].

3. TERMINOLOGY

This section provides a guide to terminology, central understanding of and adherence to the accreditation process.

- 'Accreditation Process' shall mean the necessary steps and tasks required prior to accreditation by the Security Accreditation Authority (SAA).

- 'Accreditation' shall mean the formal authorisation and approval granted to a information system by the Security Accreditation Authority (SAA) to process EU classified information in its operational environment, following formal validation of the Security Plan and its correct implementation

  The difference between these two terms is critical since it demonstrates that there are specific tasks (comprising the 'accreditation ***process'***) which must be accomplished in preparation for the formal accreditation. The tasks comprising the 'accreditation process' which are the responsibility of the System Owner (SO), whereas 'accreditation' itself is the responsibility of the Security Accreditation Authority (SAA).

- Communication and Information System (CIS) - any system enabling the handling of information in electronic form. A CIS shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources.

- Risk is measured as a combination of the likelihood of threats occurring, how vulnerable a system is to a particular threat and the impact should it occur (expressed as a value)

- Information Assurance (IA) in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, and under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authentication. IA shall be based on a risk management process.

- Risk Management - the process of identifying, assessing, treating, accepting & communicating risks.

- Classification – the process of establishing the business impacts for the Commission of a loss of confidentiality, integrity and availability of its information and of synthesising them in classification levels. The classification process is used to classify all physical and logical assets based on the classification of the information they are storing or processing (See [ASSET] and [ASSETGUIDE]).

4. ROLES AND RESPONSIBILITIES

Security related Roles and Responsibilities are based upon [844] and [3602, Annex II] However, accreditation-specific responsibilities are summarised below. The Security Plan shall identify individuals for each role (with contact details)

System Owner (SO)

The System Owner is responsible for:

- Ensuring security of the system throughout the entire life-cycle from initiation, through implementation, operation and maintenance, to withdrawal from service.
- Definition, specification and implementation of the Security Plan including security requirements and associated SecOPs as stipulated in [3602IR]
- Request for the accreditation of the system
- Tasks involved in the 'accreditation process', including development of the Security Plan and all accreditation process related documentation (See Appendix A)
- Ensuring that the system complies with corporate IT security Policies ([844], [3602]) and related Standards
- Performance of security assessments, compliance checking, inspections and reviews during the lifecycle of the CIS
- Acceptance of residual risks identified during risk management, once validated by the SAA (See Section 7.7)

Security Accreditation Authority (SAA)

The ultimate responsibility for security accreditation lies with the Security Accreditation Authority (SAA). The SAA is responsible for the approval of the security principles and requirements of the CIS system and gives the authorisation to operate the system. The SAA is will validate the formal acceptance of any residual risks by the SO identified in the risk management process.

In essence, the accreditation process consists of validation (by the SAA) of the System Owner created Security Plan. The SAA will take the formal accreditation decision, and involve the following primary roles as appropriate:

System Owner related roles:

- System Owner (SO)
- Data Owner (DO)
- LISO (associated with the System Owner's DG)

- System Security Officer (SSO)

SAA related roles:

- Crypto Approval Authority (CAA)
- TEMPEST Authority (TA)

The SAA may also involve other roles considered appropriate.

The SAA has the right to:

- require that an accreditation process be applied to a system (if not already identified as required).
- inspect or audit the system, its Security Plan and implementation against security requirements. It may do this at any point in the Accreditation Process and during the full life-cycle of the CIS.
- for existing operational systems, where secure conditions for operation are not demonstrably satisfied, require the definition and effective implementation of a Security Improvement Plan within a timescale agreed with the SAA, potentially withdrawing permission to operate the CIS until such agreement is reached.

The SAA is the Director of the Security Directorate.

Local Security Officer (LSO)

The role and responsibilities of the LSO are included in [844]. All Directorate Generals and Commission Services, including for external sites, are required to appoint at least one LSO and, if necessary, one or more deputies. In addition, inter-institutional bodies, agencies and other external entities which handle, or might handle, EU classified information (EUCI) must ensure that adequate controls and resources, including personnel, are in place to ensure its correct handling and protection.

The LSO assists the Head of every Commission Service in the discharge of his responsibility for security issues. The LSO's main function is to monitor the correct implementation of the Commission's internal security rules, as laid down in [844].

Local Informatics Security Officer (LISO)

Each Director-General or Head of Service shall appoint at least one Local Informatics Security Officer (LISO).

The role and responsibilities of the LSO (further defined in [3602]).

- shall advise and report to System Owners on information systems security matters

- shall oversee the development of the security plans approved by the Director-General and monitor their implementation
- shall contribute to awareness-raising and training programmes
- shall ensure that an inventory of all information systems is kept and updated, with a description of the security needs and a grading of the requirements
- shall ensure that IT service providers and system suppliers put in the security measures required under security plans
- Shall be involved in the checking of security incidents
- shall collaborate with the Local Security Officer (LSO) and Data Protection Coordinator (DPC)

Crypto Approval Authority (CAA)

The CAA is responsible for ensuring that cryptographic products comply with Commission's cryptographic policy in order to protect EUCI within the CIS (See [CRYPTO] and [844]).

Tempest Authority (TA)

Systems handling information classified CONFIDENTIEL UE and above shall implement countermeasures against compromising emanations and/or conductivity ("TEMPEST" countermeasures).

The TA shall be responsible for ensuring compliance of CIS with TEMPEST policies. It shall approve TEMPEST countermeasures for installations and products to protect EUCI to a defined level of classification in its operational environment

Data Owner (DO)

The DO is responsible for creation, classification, processing and use of information, including the decision as who shall be allowed to access this information.

System Security Officer (SSO)

The SSO, under the authority of the System Owner is responsible for the overall security of the system. This includes provision of the system (in a secure manner) and general system security. The SSO shall support the SO as a security expert (in combination with the LISO). The SSO is a optional role, the need for which is decided by the SO.

Security Accreditation Board (SAB)

A joint Security Accreditation Board shall provide formal advice to the Commission SAA on accreditation of Commission CIS when (parts of its) components fall under the jurisdiction of other SAAs. It shall be composed of a representative from each involved SAA and be chaired by a representative of the Commission SAA. SAA representatives from other entities with nodes on a CIS may be invited to attend when that system is under discussion. It shall act by a qualified majority of its members.

Other Roles

Other roles, specific to the system being accredited, will be necessary on a case by case basis (e.g. system helpdesk, network service provider(s), system administrators, etc). The Security Plan shall identify such roles, the individuals that perform them, and contact details as appropriate.

5. DESIGN PRINCIPLES

System Owners should note that, in line with current best practice, particular attention shall be paid to the following principles:

- Need to Know - meaning that an individual shall only have access to information necessary to perform their function or task. Access to EU classified information shall be authorised only for persons having a 'need-to-know' for carrying out their duties or missions
- Minimality – only the essential functionalities, devices and services to meet operational requirements shall be implemented in order to avoid unnecessary risk
- Least Privilege – users and automated processes shall be given only the access, privileges and authorisations required to perform their tasks
- The 'four eyes' principle - for particularly sensitive operations there are always two individuals involved with the action

The following items, in particular, shall form mandatory considerations as input to the accreditation process:

- Interconnection of networks and boundary protection – that interconnections are subject to risk analysis leading to effective countermeasures and approval by the SAA and any other appropriate parties. CIS shall treat any interconnected IT system, by default, as untrusted and shall implement protective measures to control the exchange of classified information
- Physical security of premises (sites, buildings and areas within buildings) and accredited CLASS I security areas for CIS handling CONFIDENTIEL UE or above
- Industrial security: External contractors shall have appropriate security clearances relating to the EUCI handled.
- Personnel operating CIS handling EUCI shall be security cleared
- Use of TEMPEST equipment to protect against electronic eavesdropping by interception of electromagnetic emanations (this is only relevant for CIS handling information classified CONFIDENTIEL UE or above)
- Use of appropriate and certified cryptographic measures to protect confidentiality and integrity of data at rest and during transmission (See [844] and [CRYPTO])
- Disaster Recovery/Business Continuity Planning
- Testing of the systems security functionality and vulnerability testing

- System Technical documentation: Detailed description and explanation of the technical aspects of the system (e.g. architecture, network topology, platforms, infrastructure, software, configuration, acceptance criteria for components)

- Implementation of appropriate logging and tracing

6. PRINCIPLES OF THE SECURITY ACCREDITATION PROCESS

The accreditation process is based on the following principles:

- The 'legal base' and underlying principles for the Security Accreditation Process are contained in [844], [3602] and [3602IR]

- The Accreditation Process (tasks required prior to formal accreditation) is a structured risk based approach ensuring that the Security Plan has been derived appropriately, is fit for purpose and is correctly implemented.

- Accreditation relies on formal validation of a system's Security Plan (See [3602IR]).

- This document describes the minimum steps and level of documentation required during the Accreditation Process. The precise process will vary for each system and guidance shall be sought from the SAA and applied accordingly.

- The SAA will inspect the system, its Security Plan and implementation against security requirements as part of its duty, and may do this at any point in the Accreditation Process.

- The aim of Risk Treatment shall be to apply a set of security measures which results in an appropriate balance between requirements, cost and residual security risks. This principle applies to appropriate accreditation effort, taking account of relevant factors, including the classification level of the EUCI handled in the CIS.

- The [3602IR] Plan-Do-Check-Act approach shall be applied for the implementation of the information systems security policy during the full life-cycle of the information system

- To mitigate risk, security measures (technical and non-technical) shall be organised as multiple layers of defence. These layers include:

    - Deterrence: security measures aimed at dissuading an adversary planning to attack the CIS

    - Prevention: security measures aimed at ensuring attacks fail due to the implementation of security measures

    - Resilience: security measures aimed at limiting the impact of an attack to a minimum set of information or CIS assets and preventing further damage

    - Recovery: security measures aimed at regaining a secure situation for the CIS

  The degree of stringency of such measures shall be determined following a risk assessment

7. DEFINITION OF THE SECURITY ACCREDITATION PROCESS

The Accreditation Process consists of the following sequential tasks. The documentation produced during each task shall form part of the Security Plan for the system (either directly or through reference from it). The System Owner shall be responsible for the production, approval and classification of the documentation.

In essence, the accreditation process consists of validation (by the SAA) of the System Owner created Security Plan. Also see [3602IR, Section 3.4]. Any deviation from the Accreditation Process defined in this document shall be requested from the SAA who will consider the case for exception. Details shall be fully documented and justified (in the System Accreditation Strategy (SAS)) by the System Owner (SO).

See Appendix A for a full list of Accreditation Process documentation.

7.1. Request Security Accreditation

The System Owner shall formally request that the system be subject to accreditation by the SAA. The System Owner should wait for acceptance of this request from the SAA prior to the next Accreditation Process step.

7.2. Define the system scope

The security related scope and boundaries of the system must be defined by the system owner in terms of various characteristics, including:

- System role/functionality
- Roles and responsibilities
- User types, including numbers
- Locations
- Mode of Operation
- Assets (information and otherwise), including type, volume and summary of classification
- Technical details (e.g. architecture, network topology, platforms, infrastructure, software, interconnections, etc)
- Legal, regulatory and contractual frameworks
- Assumptions and Constraints

For further information see [3602IR, Annex A– Part 1], [SPGUIDE, Section 2] and [ASSET, Section 3]

The scope documentation shall require approval by the SAA prior to the next Accreditation Process step. The SAA will check the completeness and consistency of the system scope both within the document and with relevant IT security policy.

7.3. Define the System Accreditation Strategy (SAS)

The System Accreditation Strategy (SAS) for the CIS shall define any system-specific accreditation strategy details (where they deviate from or augment this process), including accreditation roles and responsibilities. The SAS shall be produced by the Security Accreditation Authority in agreement wit the System Owner.

The SAA will ensure the completeness and consistency of the System Accreditation Strategy both within the document and with relevant IT security policy, such as this standard.

7.4. Define the Security Needs/Perform Business Impact Assessment

The security needs of the information system must be established using a Business Impact Assessment (BIA) process. This task establishes the security needs of the system/data in terms of confidentiality, integrity, availability[1].

Descriptions of the classification levels of data, categories of information systems (SPECIFIC or STANDARD), designators and markings of information are provided in [3602, Section 3.4], [3602IR, Annex I], [ASSET] & [SN1].

The Security Needs/BIA documentation shall require approval by the SAA, prior to the next Accreditation Process step.

7.5. Perform Threat and Vulnerability Assessment

As input to the risk assessment, it is necessary to consider:

- The level of various threats to assets – i.e. how likely a given type of threat is to occur

- The extent to which assets are vulnerable to certain threats (i.e. ignoring the likelihood of a threat occurring, would a particular asset be impacted greatly or not)

Each system shall perform a Threat and Vulnerability (T&V) assessment to determine the above. The T&V assessment shall adhere to a risk assessment methodology agreed with the SAA (e.g. CRAMM, EBIOS) and be documented in the System Accreditation Strategy (SAS). It shall be consistent with the policy on risk management ([3602IR, Section 4]).

[1] Destruction and repudiation shall also be considered

7.6. Perform Risk Assessment

The security aspects of the system shall be modelled using the system definition (scope), assets, BIA and T&V assessment. This enables a risk assessment to be performed, resulting in:

- A prioritised list of risk areas, showing the level of risk in each area
- A list of security countermeasures based on the Business Impact Assessment (BIA) and T&V assessment.

The complete set of proposed *initial security countermeasures* for the system shall comprise of:

- 'Baseline security material' ([3602], [3602IR], [SN1] and mandatory security standards)
- Additional Countermeasures derived from the risk assessment
- Requirements or standards which may be specific to the system (e.g. security standards for smartcards, radio transmission standards for hand held security device, mobile phone OS standards, etc)

Using the information resulting from the risk analysis the System Owner shall produce a Risk Report which includes:

- a summary of the risk assessment methodology used (including specifics involved for this system)
- the prioritised list of risk areas, justification & comments for the assigned priorities
- supporting information regarding the security model[2].

The principles of risk management are given in [3602IR, Section 4].

The Risk Assessment documentation, including the Risk Report, and risk assessment methodology used shall require approval by the SAA, prior to the next Accreditation Process step.

[2] Throughout the risk assessment process a model of the security aspects of the CIS is formed. This includes all relevant components that must be considered (e.g. assets, interactions between them, impact considerations, threats, vulnerabilities, risks, environment factors)

7.7. Definition of Security Requirements and Risk Treatment

The initial security requirements shall undergo Risk Treatment to derive the *definitive security countermeasures* to be implemented for the system. This involves considering the prioritised areas of risk and the initial security countermeasures to consider the appropriate risk treatments. Options for treatment are (combinations of):

- Reduce (implement identified countermeasures)
- Accept (consider the level of risk to be acceptable and not implement countermeasures)
- Transfer (move management and responsibility of the risk to another party)
- Avoid (remove the source of the threat to the system such that the risk no longer applies)

A Risk Treatment Plan (RTP) shall consider all areas of risk and countermeasures identified in the Risk Analysis (see Section 7.6), denoting what treatments shall be applied.

The RTP shall identify (theoretical) residual risks in a Residual Risk Statement in the Security Plan (i.e. those risks which are not fully treated, transferred or avoided). The Residual Risk Statement shall undergo formal validation by the SAA (in concert with the System Owner). Areas of risk accepted and countermeasures that are not selected for implementation (fully or partially) and the reasons and justifications for this decision shall be described in the Residual Risk Statement.

The Security Plan shall detail any compensating controls, which may (when justified) replace countermeasures contained in the set of initial security countermeasures.

The definitive security requirements, Risk Treatment Plan and Residual Risk Statement shall require approval by the SAA, prior to the next Accreditation Process step.

7.8. Security Implementation Plan

Once the definitive security requirements for the system have been derived, a Security Implementation Plan (SIP) shall be documented to ensure effective implementation of the Security Plan[3]. This shall include:

- Identification of appropriate management action
- Definition of the security measures to be implemented to mitigate identified risks
- Identification of resource/cost requirements
- Identification of training and awareness requirements
- Identification of responsibilities and priorities for managing the implementation
- Identification of security related software and hardware replacement (with a definition of what would be considered 'significant' changes – See Section 7.12)
- Identification of the full security documentation set (including SecOps), existing or planned for production, which will be used to implement and operate security of the system.

The Security Implementation Plan shall require approval by the SAA, prior to the next Accreditation Process step.

7.9. Security Audit

A Security Audit shall be performed by the SAA to determine the extent to which the Security Plan, through its Security Implementation Plan, has been correctly and fully implemented. The scope of this audit will be determined by the SAA and will be dependant on the scope and complexity of the system, and the classification of its data.

The Security Audit is the responsibility of the SAA (with information provided by the SO, as necessary).

[3] In fact, the SIP is ***one of*** the set of documents which make up the overall Security Plan. It's purpose is to describe how the other parts shall be derived.

7.10. Formal Accreditation

Following the preceding accreditation process steps, formal Accreditation of the system by the SAA may occur.

Following the preceding steps of the accreditation process, the SAA will decide whether to formally accredit the system. The accreditation process will result in one of the following:

(1) A **Deny Approval to Operate**, if the level of residual risk is deemed too high or if critical security measures, including the appropriate documentation, are not implemented. Note that where the system is an existing live system this would represent an instruction to remove authorisation for handling of EUCI or operation of the system until certain measures have been implemented.

(2) An **Interim Approval to Operate**, if the level of residual risk is acceptable and if some security measures, including the appropriate documentation, are not yet implemented. This interim approval can only be given if a plan for the improvement of security leading to the full approval is available and accepted by the SAA.

(3) **Full Approval to Operate**, if the level of residual risk is acceptable and all appropriate security measures, including the appropriate documentation, are implemented.

The accreditation decision shall define the maximum EU classification level of the information that may be handled by the system and corresponding limitations and conditions for the validity of the accreditation being granted. This shall include a statement regarding the time limit which the accreditation decision is valid for.

7.11. Communication to Stakeholders

Following formal accreditation of the system the SO shall ensure all relevant stakeholders (i.e. those individuals identified in Section 4 and others as considered appropriate by the SO) have been informed of the accreditation verdicts. The SAA shall inform the relevant services in member states.

7.12. Accreditation Maintenance and Validity

Once granted, an accreditation of a system is valid until one of the following occurs:

- The time limit which the accreditation decision is valid for is reached (accreditation expiration)
- An audit (or similar compliance check) identifies that the Security Plan (including the security countermeasures defined by it) is not being effectively implemented or adhered to
- A major security incident

- There is a change to in the characteristic of the system, significant enough to required revisit of the Accreditation.

'Significant changes' include:

- Reassignment of System Ownership
- change in the information system architecture
- changes to the system's software (including bug fixes and patches) or hardware replacement. The definition of what would be considered 'significant' changes shall previously be defined in the SIP (See Section 7.8)
- change of scope, assets or CIA profile (including the EUCI levels handled by the system)
- additions/deletions of system interconnections

Under such circumstances the SAA shall be consulted and appropriate tasks defined to ensure appropriate revisit/reapplication of the Accreditation Process (including reassessment of the accreditation validity period). The SAA shall be kept informed of all changes and can also decide whether a change be considered 'significant' and therefore requires reconsideration of the accreditation status.

Throughout the lifetime of the system, security audits may be performed by the SAA to ensure continued adherence to the security plan, and effectiveness of that plan. Such audits will consider all deployed measures and site locations.

At a minimum the Security Plan shall be reviewed, updated and its correct implementation checked annually by the System Owner.

Annex

Appendix A Accreditation Process Documentation

The accreditation process requires that material stated in the following table be created prior to formal accreditation by the SAA.

The following documents make up the overall Security Plan:

Accreditation Process Material – Security Plan		
Document	**Description**	**Described in**
Security Plan document	The top level document used to organise all other accreditation deliverables. Guidance on Security Plan content can be found in [SPGUIDE]	Throughout Section 7
Scope	Defines the security related scope of the system and accreditation strategy	7.2
System Accreditation Strategy	System-specific accreditation strategy details (where they deviate from or augment this process), including accreditation roles and responsibilities	7.3
Business Impact Assessment	Security Needs of the system/data in terms of confidentiality, integrity, availability	7.4
Threat and Vulnerability	Threat and vulnerability information as appropriate according to the Risk Assessment method used.	7.5
Risk Report	includes: • a summary of the risk assessment methodology used • definition of the assets included in the risk assessment • the prioritised list of risk areas, justification & comments for the assigned priorities • supporting information regarding the security model (such as asset groupings and notes regarding the risk model) • residual risk statement	7.6
Risk Treatment Plan	Maps risk areas and security countermeasures identified in the risk analysis to the manner in which they shall be treated	7.7
Definitive security Countermeasures	Security countermeasures resulting from risk analysis and risk treatment process	7.7
Security Implementation Plan	Documents required measures to ensure effective implementation of the Security Plan	7.8

In addition to the above items created during Accreditation Process phases, the security countermeasures will be expressed in various other documentation (e.g. SecOPs). The System Owner shall determine the appropriate documentation set for their system. It shall include, but is not limited to, the following

Other Security Material Necessary for Accreditation	
Disaster Recovery/Business Continuity Plan	Provides details regarding how the system would operate should a disaster occur at sites associated with the system, ensuring appropriate levels of system continuity and restoration. This shall also cover appropriate emergency procedures (e.g. to counter risk for civil disturbance, cyber attack, etc) including emergency destruction of EUCI equipment and material.
System-specific Interconnection Security Requirement Statement (SISRS). document	Connections between external networks and the system will be mediated by a System-specific Interconnection Security Requirement Statement (SISRS). This will address the security rules/network defence measures which need to be in place between two networks which connect up (i.e. requirements on both sides) and the mechanism for agreeing how such connections will be authorised.
Security awareness material	This shall ensure that all staff are fully aware of their responsibilities for information security, and may require material specific to the system
Security Incident Management scheme	Users of the system shall follow a Security Incident Management scheme
Security Testing Strategy including Vulnerability Testing	Security testing of countermeasures (technical and non-technical) during the Accreditation Process to ensure that the appropriate level of assurance is obtained and correct implementation, integration and configuration. Security testing shall include (but is not limited to): • Security Test Plan • Vulnerability Testing • Process for identification known vulnerabilities in system components • Functional testing of secure aspects • Introduction of new functionality (change management) • Approach to upgrades and bug fixes • Testing results
System Technical documentation	Detailed description and explanation of the technical aspects of the system (e.g. architecture, network topology, platforms, infrastructure, software, configuration, acceptance criteria for components)
Cryptographic documentation	Detailed description of all cryptographic aspects of the system (e.g. key generation, distribution, destruction, etc)

TEMPEST documentation	Description of how applicable TEMPEST policies are complied with.
SecOPs	Detailed procedures used for day to day implementation/operation of security. Examples are: • Roles and responsibilities (including segregation of duties information) • Procedure to be used to demonstrate compliance to security • Criteria applying to third parties (e.g. required security clearance, service level agreements, definition of services supplied). • Physical and secure area security procedures • Handling of removable media • Analysis of audit logs • Media sanitisation, destruction and reuse procedure • Backup • Secure system maintenance • Virus and Malware procedures • User registration/deregistration procedure • Rules for the acceptable use of information and assets (an "Acceptable Use Policy (AUP)") • Security clearance of individuals procedures • Documentation handling procedure (linked to marking/classification information) • Coding standards • Data Migration procedures • Data Transfer procedures • Acceptance into Service (AiS) procedures
Security related Service Records	The system will be supported by various records and service logs. Examples include: • Document/Code review/sign-off records • Test review/sign-off records • User access/privilege request forms • Audit records • Traceability matrices • Site/room visitor books • Minutes of security related meetings • Change management records • Risk sign-off records • Destruction/sanitisation records • Maintenance records • Clearance checking evidence • Receipts for received deliveries • Administrator log books

Various mappings to allow maintenance of the system security model.	Through the Security Accreditation Process documentation will be created to describe methods used, assumptions made and mappings to ensure completeness. These need maintaining to allow use in the future and to check Risk Assessment conclusions

Note that the manner of which the material is expressed is not mandated. For example, the Risk Treatment Plan (RTP) may be expressed in a document or a spreadsheet. The manner in which material is expressed shall be described in the Security Plan.

Appendix B Acronyms, and Abbreviations

Item	Description
IA	Information Assurance
BIA	Business Impact Assessment
CAA	Cryptographic Approval Authority
CIS	Communication and Information Systems
CRAMM	A risk assessment methodology
DO	Data Owner
Document	Any letter, note, minute, report, memorandum, signal/message, sketch, photograph, slide, film, map, chart, plan, notebook, stencil, carbon, tape, computer disk, CD-ROM, DVD or other physical medium on which information has been recorded
EC	European Commission
EUCI	European Union Classified Information
LISO	Local Informatics Security Officer
Mode of Operation	The Mode of Operation of a system defines the extent to which users of a system are authorised to access information held on the system and their need to know that information. The security operating mode of the system is defined as one of the following categories: • Category 1: exclusive operating mode: Everyone accessing the system is authorised for the highest classification level and has an identical need to know (or equivalent) with regard to all the information processed, stored or sent by the system. • Category 2: dominant operating mode: Everyone accessing the system is authorised for the highest classification level but they do not have an identical need to know (or equivalent) with regard to the information processed, stored or sent by the system. • Category 3: multilevel operating mode: Not everyone accessing the system is authorised for the highest classification level and they do not all have an identical need to know (or equivalent) with regard to the information processed, stored or sent by the system.

Item	Description
RTP	Risk Treatment Plan
SAA	Security Accreditation Authority
SO	System Owner
SSO	System Security Officer
SIP	Security Implementation Plan
SecOP	Security Operating Procedure
TA	TEMPEST Authority

Appendix C References

Policies:

Reference	Document
(1) 3602	Commission Decision of 16 August 2006 C(2006) 3602 concerning the security of information systems used by the European Commission
(2) 3602IR	Implementing Rules for Commission Decision C(2006) 3602 of 16.8.2006 concerning the security of information systems used by the European Commission, Adopted 29/05/2009
(3) 844	Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure (notified under document number C(2001) 3031) (OJ L 317,3.12.2001, p.1) as amended by: • Commission Decision 2005/94/EC, Euratom, of 3 February 2005 (OJ L 31, p.66, 4.2.2005); • Commission Decision 2006/70/EC, Euratom, of 31 January 2006 (OJ L 34, p.32, 7.2.2006); • Commission Decision 2006/548/EC, Euratom, of 2 August 2006 (OJ L 215, p.38, 5.8.2006); adopting the Commission provisions on security.
(4) SN1	Security Notice 1 - The use and application of security designators and markings

Standards:

Reference	Document
(5) CRYPTO	European Commission Information System Security Policy: C(2006) 3602 – Draft Standard on Cryptography and Public Key Infrastructure, Dated 23/08/2010
(6) ASSET	European Commission Information System Security Policy: C(2006) 3602 Standard on Asset Management Dated 28/05/2010

Guidelines:

Reference	Document
(7) ASSETGUIDE	European Commission Information System Security Policy: C(2006) 3602 - Guidelines on Asset Classification, Dated 09/10/2009
(8) SPGUIDE	C(2006) 3602 Guidelines on Security Plan, dated 03/05/2010