TECHNICAL REPORT

ISO/IEC TR 19791

First edition
2006-05-15

Information technology — Security techniques — Security assessment of operational systems

Technologies de l'information — Techniques de sécurité — Évaluation de la sécurité des systèmes opérationnels

Reference number
ISO/IEC TR 19791:2006(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 19791, which is a Technical Report of type 2, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

The technical content of this Technical Report has been published as a Common Criteria Supporting Document by the Common Criteria Development Board.

Introduction

This support document defines extensions to ISO/IEC 15408 to enable the security assessment (evaluation) of operational systems. ISO/IEC 15408, as currently defined, provides support for specifying the IT security functionality that exists in products and systems. However, it does not capture certain critical aspects of an operational system that must be precisely specified in order to effectively evaluate such a system.

This Technical Report provides extended evaluation criteria and guidance for assessing both the information technology and the operational aspects of such systems. The document is primarily aimed at those who are involved in the development, integration, deployment and security management of operational systems, as well as evaluators seeking to apply ISO/IEC 15408 to such systems. It will be relevant to evaluation authorities responsible for approving and confirming evaluator actions. Evaluation sponsors, and other parties interested in operational system security, will be a secondary audience, for their background information.

Considering the complexity of this project and the need for additional work, the target has been defined to be a type 2 Technical Report. In the future, once additional experience has been gained in this area, it is hoped that it may be possible to convert this Technical Report into an International Standard to support ISO/IEC 15408 specifically for evaluations of operational systems. Until some formalisation of an approach is performed, it is considered unlikely that many operational system evaluations of this nature will be undertaken due to the lack of specific guidance available, a gap that this TR is designed to fill.

There are fundamental issues in regard to the definition and use of the term *system*. ISO/IEC 15408, with its focus on product evaluation, uses the term to include only the information technology (IT) aspects of the system. The term *operational system*, as used within this Technical Report, covers the combination of personnel, procedures and processes integrated with technology-based functions and mechanisms, applied together to establish an acceptable level of residual risk in a defined operational environment.

Information technology — Security techniques — Security assessment of operational systems

1 Scope

This Technical Report provides guidance and criteria for the security evaluation of operational systems. It provides an extension to the scope of ISO/IEC 15408, by taking into account a number of critical aspects of operational systems not addressed in ISO/IEC 15408 evaluation. The principal extensions that are required address evaluation of the operational environment surrounding the TOE, and the decomposition of complex operational systems into security domains that can be separately evaluated.

This Technical Report provides

a) a definition and model for operational systems;

b) a description of the extensions to ISO/IEC 15408 evaluation concepts needed to evaluate such operational systems;

c) a methodology and process for performing the security evaluation of operational systems;

d) additional security evaluation criteria to address those aspects of operational systems not covered by the ISO/IEC 15408 evaluation criteria.

This Technical Report permits the incorporation of security products evaluated against ISO/IEC 15408 into operational systems evaluated as a whole using this Technical Report.

This Technical Report is limited to the security evaluation of operational systems and does not consider other forms of system assessment. It does not define techniques for the identification, assessment and acceptance of operational risk.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1:2005, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:2005, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*

ISO/IEC 15408-3:2005, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*

3 Terms and definitions

For the purposes of this document, terms and definitions given in ISO/IEC 15408-1:2005 and the following apply.

3.1
component
identifiable and distinct portion of an operational system that implements part of that system's functionality

3.2
external operational system
separate operational system which interfaces to the operational system that is the subject of evaluation

3.3
management controls
security controls (i.e., safeguards and countermeasures) for an information system that focus on the management of risk and the management of information system security

[NIST SP 800-53]

3.4
operational controls
security controls (i.e., safeguards and countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems)

[NIST SP 800-53]

3.5
operational system
information system, including its non-IT aspects, considered in the context of its operating environment

3.6
residual risk
risk that remains after risk treatment

[ISO/IEC 13335-1:2004]

3.7
risk
potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

NOTE Risk is measured in terms of a combination of the probability of an event and its consequence.

[ISO/IEC 13335-1:2004]

3.8
risk analysis
systematic approach of estimating the magnitude of risks

[ISO/IEC 13335-1:2004]

3.9
risk assessment
process of combining risk identification, risk analysis and risk evaluation

[ISO/IEC 13335-1:2004]

3.10
risk management
total process of identifying, controlling and eliminating or minimizing uncertain events that may affect system resources

NOTE Adapted from ISO/IEC 13335-1:2004. Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication (exchange or sharing of information about risk between the decision-maker and other stakeholders).

3.11
risk treatment
process of selection and implementation of security controls to modify risk

NOTE Adapted from ISO/IEC 13335-1:2004.

3.12
security controls
management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information

[NIST SP 800-53]

NOTE This definition is intended to include controls that provide accountability, authenticity, non-repudiation, privacy and reliability, which are sometimes considered as distinct from confidentiality, integrity and availability.

3.13
security domain
portion of an operational system that implements the same set of security policies

3.14
subsystem
one or more operational system components that are capable of execution separately from the rest of the system

3.15
system target of evaluation
operational system that is being operated in accordance with its operational guidance, including both technical and operational controls

NOTE Operational controls form part of the operational environment. They are not evaluated in ISO/IEC 15408 evaluation.

3.16
technical controls
security controls (i.e., safeguards and countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system

[NIST SP 800-53]

3.17
verification
assessment processes used to confirm that the security controls for an operational system are implemented correctly and are effective in their application

3.18
vulnerability
flaw, weakness or property of the design or implementation of an information system (including its security controls) or its environment that could be intentionally or unintentionally exploited to adversely effect an organization’s assets or operations

4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 15408-1:2005 and the following apply.

COTS	Commercial Off The Shelf
ETR	Evaluation Technical Report
ISMS	Information Security Management System
OSF	Operational Security Functionality
SP	Special Publication
SPP	System Protection Profile
SSA	System Security Assurance
SSF	System Security Functionality
SST	System Security Target
STOE	System Target of Evaluation

5 Structure of this Technical Report

Clauses 1 to 4 contain introductory and reference material, and are followed by this overview of the contents of the Report (Clause 5).

Clause 6, *Technical approach*, describes the technical approach to operational systems assessment used in this Technical Report.

Clause 7, *Extending ISO/IEC 15408 evaluation concepts to operational systems*, describes how ISO/IEC 15408 evaluation concepts have been extended for use in operational system evaluation.

Clause 8, *Relationship to existing security standards*, describes the relationship between this Technical Report and other security standards which have been used in its development.

Clause 9, E*valuation of operational systems*, contains requirements for specification of security problems, security objectives, security requirements, SST contents and periodic reassessment which are needed in order to evaluate operational systems.

Annex A, *Operational system Security Targets and System Protection Profiles*, defines the security requirement specifications needed for operational systems.

Annex B, *Operational system functional control requirements*, defines the additional security functional requirements needed for operational systems.

Annex C, *Operational system assurance requirements*, defines the additional security assurance requirements needed for operational systems.

Annex D, *Relationship to Common Criteria development*, identifies necessary differences between the evaluation of operational systems and product evaluation based upon proposed changes to the Common Criteria.

6 Technical approach

6.1 The nature of operational systems

For the purposes of this Technical Report, an operational system is defined as an information system, including its non-IT aspects, considered in the context of its operating environment.

Many operational systems are complex in nature, made up of a combination of subsystems that are partially proprietary and unique in nature, and partially constructed using bought-in general products. They interact with and have dependencies upon other systems. An operational system is typically built using components from multiple vendors. These components may be integrated to compose the operational system by an integrator that does not perform any development functions, only configuration and interconnection.

However, operational systems typically:

— are under the control of a single entity, the operational system owner;

— are built against specific needs, for a specific type of operation;

— change frequently; either in technical set-up and/or in operational requirements;

— contain a considerable (or even large) number of components;

— contain bought-in components that possess a large number of possible configuration alternatives;

— enable the operational system owner to balance technical (and specifically IT) and non-technical security measures;

— contain components with different degrees and types of security assurance.

6.2 Establishing operational system security

Secure products offer an important contribution to operational system security and indeed the use of products evaluated against ISO/IEC 15408 may be preferable in construction of a secure operational system. However, security problems in operational systems are caused not only from product problems but also from operational system problems in a real operational environment, such as poor application of bug fixes, poor setting of access control parameters or filtering rules of a firewall, poor linking of files directories, etc. Furthermore, in the case of a network, the security level of an operational system connected to the network might be of concern to other operational systems that have to communicate with it.

This Technical Report is based upon a three step approach to establishing the necessary level of security for an operational system:

a) risk assessment, to determine the security risks applicable to a system;

b) risk reduction, to counter or eliminate security risks by the selection, application and assessment of security controls;

c) accreditation, to confirm that the residual risks remaining within the system after the controls are applied are appropriate for the system to be used in live operation.

Conceptually, this three step process is shown in Figure 1 following.

This Technical Report addresses only the middle step of the three step process, namely risk reduction through the selection, application and assessment of security controls. To do this, it uses a security evaluation approach, based upon the security evaluation model for IT security controls defined in ISO/IEC 15408, but extended to deal with all types of security controls.

Techniques and methods for risk assessment are beyond the scope of this report. For more information on risk assessment, see part 3 of ISO/IEC 13335 [1].

NOTE Note that part 3 of ISO/IEC 13335-3 is a Technical Report. International Standard ISO/IEC 27005, when published, will supersede ISO/IEC TR 13335.

Techniques and models for accreditation are a management responsibility, beyond the scope of this report. For more information on one possible approach, see NIST SP 800-37 [2].

The security evaluation model of ISO/IEC 15408 excludes consideration of the operational environment surrounding the IT portion of the information system. The operational environment is treated as assumptions in ISO/IEC 15408 evaluation, but cannot be discounted for operational systems. Typically, operational systems are reliant on non-IT security measures, e.g. measures of an administrative or physical nature. There is therefore a need to define ways to express and evaluate such requirements and controls, as an extension to the ISO/IEC 15408 specification criteria. This Technical Report extends ISO/IEC 15408 to do this.

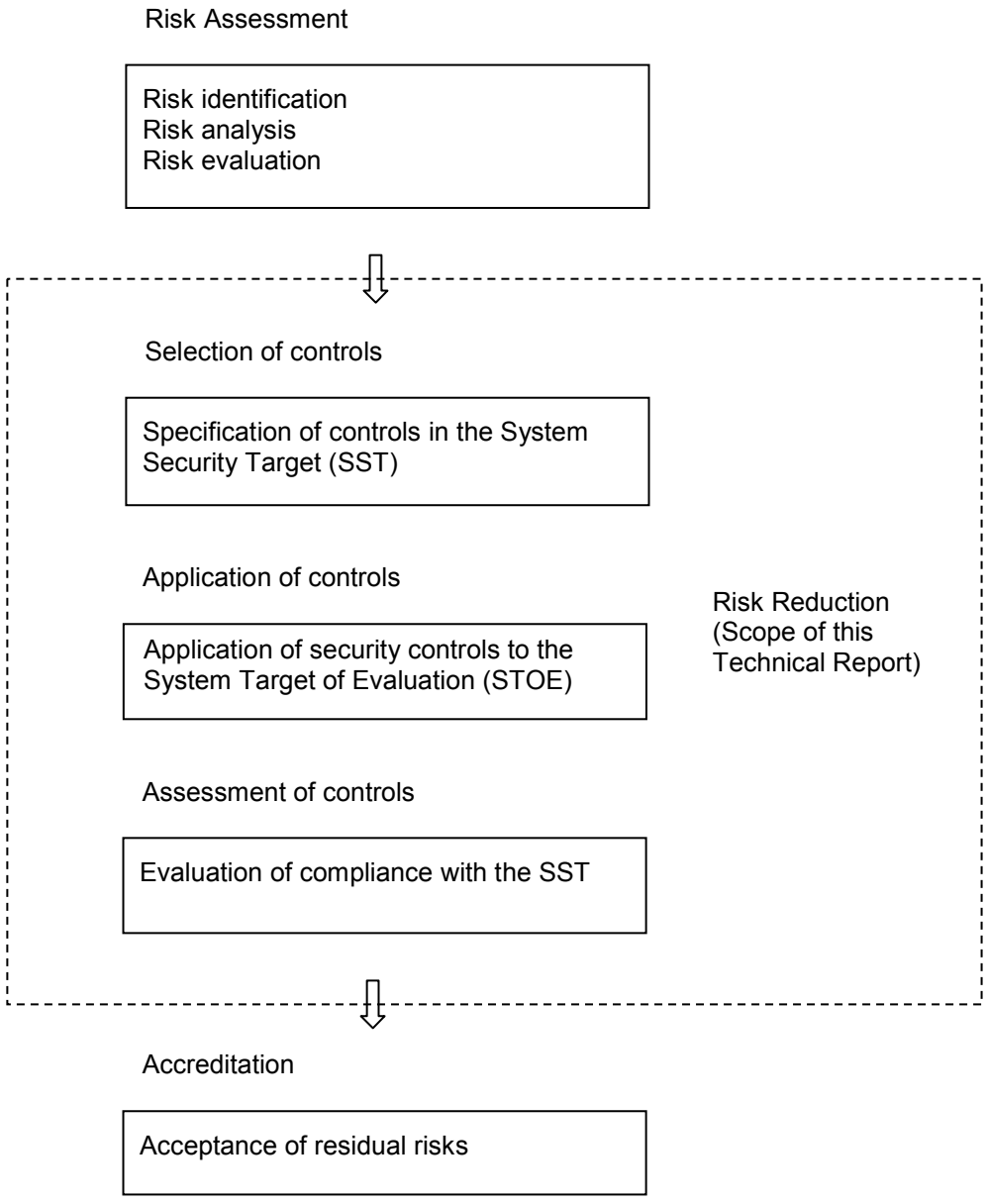

Figure 1 — Process for establishing operational system security

In total, the extensions to ISO/IEC 15408 within this Technical Report include, but are not limited to:

a) Positioning security evaluation within an overall methodology for the security assessment of operational systems including their operational environment.

b) A methodology for specifying the internal structure of operational systems, including details of internal and external interfaces, to the extent necessary to understand how the various portions of an operational system interoperate.

c) A catalogue of assurance criteria to express the extensions to the scope of evaluation (see Annex A).

d) A catalogue of functional criteria to express additional operational security controls (see Annex B).

e) A catalogue of assurance criteria to express the additional evaluation tasks needed to assess operational systems (see Annex C).

Extending the ISO/IEC 15408 approach to the evaluation of complete operational systems has the advantage of using a defined existing metric so that common and mutual understanding of evaluation results is possible. For a specific operational system, advertising the evaluation result in a way that is compatible with ISO/IEC 15408 might bring business advantage to customers, not only for service provider systems such as internet banking systems, but also from the view point of social responsibility.

Operational system evaluation requires that a prior risk assessment has identified the security risks applicable to an operational system, and determined those risks that are unacceptable and must be reduced or eliminated through technical and operational controls. It then consists of the following steps:

a) Setting security objectives for the operational system that will reduce the unacceptable risks to a level which is tolerable.

b) Selecting and specifying technical and operational security controls that satisfy the security objectives for the operational system, taking due account of controls that already exist.

c) Defining concrete, measurable assurance requirements for both the technical and operational controls to gain the requisite level of confidence that the operational system meets its security objectives.

d) Recording the decisions made in a System Security Target (SST).

e) Evaluating the actual operational system to judge compliance with the SST.

f) Periodically reassessing both the security risks to the operational system and the operational system's ability to address those risks.

Although this model is an extension of the ISO/IEC 15408 model, it is consistent with that model so that ISO/IEC 15408 evaluation results can be reused.

6.3 Security in the operational system life cycle

6.3.1 Overview

The life cycle of an operational system is considered to have four phases, namely development/integration, installation, system operation and modification. The security controls of an operational system must be assessed throughout the lifetime of the system.

6.3.2 Development/integration phase

During the development/integration phase, the first security activity is to identify the risks to the operational system. Those risks that are considered unacceptable must be reduced or eliminated by security measures built into the system. Following the risk assessment and identification of risks to be eliminated, an authorized officer of the organization, the Accreditor, must consider the anticipated residual risks, and the sum of the residual risks, and confirm that they will be acceptable.

The operational system will then be designed, including the use of software and hardware products, the physical facilities required, the business application programs needed and the technical security controls required. The design of the operational system must be recorded in the SST. The SST will contain a description of the system security requirements, including the risks to be countered and the security objectives to be achieved by technical and operational controls. The list of technical and operational controls documented in the SST will represent an instantiation of the system security objectives.

For the purposes of correctness, security objectives should be specified in the SST that address all risks identified as unacceptable. The SST should specify security requirements that completely satisfy the security objectives without any additions or omissions. The design documentation for the operational system should identify precise security countermeasures within the operational system that meet all of the security requirements specified in the SST. The countermeasures might be security functions, facilities, procedures or rules. The countermeasures should be adequately controlled, managed and applied to the system. The security countermeasures should be implemented without any unauthorized addition, elimination or modification. The implementation should be verified with testing of the system or checking of documents. The operation of security countermeasures should be adequately described in the guidance documents.

For effectiveness, the selected security requirements should reduce all security risks identified by risk assessment as unacceptable to a level that can be tolerated as residual risks. Each security countermeasure should work effectively in combination with other countermeasures to satisfy the overall security requirements for the operational system. The strength of the security mechanisms should be sufficient to match the expected attack potential. Vulnerability analysis and penetration testing might be required with the expected attack potential.

Evaluators should be involved in the development/integration phase, early in the system life cycle, to facilitate their understanding of the system and its intended environment, as well as to provide input from review of design documentation, and to provide guidance on evaluation and guidance documentation to be used as part of assurance evidence. Ideally the full SST should be evaluated in a preliminary evaluation to confirm that there are no inconsistencies or omissions in the security requirements and proposed controls.

The business applications and systems software, including the technical security controls, are then produced or purchased, and the system is integrated, configured, and tested by the developer. At the same time, the operational security organization is created and security policies, rules and procedures produced and integrated into the system. The proper security configuration settings should be identified and implemented.

Following integration testing, the operational system should be security tested as part of the developer's requirements verification testing. Typically, system specific security controls such as access controls can be verified by the developer prior to deployment at the operational site. Testing of site specific security controls (both technical and operational) is deferred until the system is installed in its intended operational environment. Verification testing will confirm the strength of security mechanisms, as well as the correct operation of the security controls.

The operational system will then be evaluated. The evaluation should confirm that all risks, as detailed in the SST, that have to be countered by security controls are addressed by the system at an acceptable level. The result of the evaluation is an independent confirmation to the system owner that this is the case.

The Certification Report will list any confirmed vulnerabilities found in evaluation, and identify any recommended corrective actions, as required. The system owner will then prepare a corrective action plan to reduce or eliminate the identified vulnerabilities, as deemed appropriate. The result of the certification of the system will be presented to the Accreditor for determination that the actual residual risk to operations and system assets is acceptable. The output of this phase will be an authorization for the system to operate.

6.3.3 Installation phase

During the installation phase, the technical and operational controls will be implemented and prepared for use in the operational environment. Site specific controls will be tested, and other controls retested to confirm that they perform correctly in the actual operational environment.

For the purposes of correctness, the controls should be compliant with the security requirements documented in the SST and authorized for use by a competent person. To be effective, all persons should be trained in use of the security controls and procedures.

6.3.4 System operation phase

In the system operation phase, records of the operation of technical controls and operational controls should be collected and assessed. Audit trails and monitoring records for all access to assets should be logged. Security countermeasures should be confirmed as operating as intended. It should be verified that unauthorized operations and unacceptable risks have not occurred. Secure states should be recovered from insecure states within the required time. Changes due to routine maintenance should be monitored and assessed for security problems. Records of actual access and utilization of assets should be inspected. Security problems should be reported, reviewed and analyzed.

The purpose of these activities is to provide feedback to the Accreditor when changes occur that may have an impact on operational system security. Typically, in systems operation, a critical subset of the operational system security controls should be identified for regular monitoring to determine their continued effectiveness. Additionally, the system owner should have in place a configuration management, control, and reporting system that documents the current operational system assets, its configuration, and presents that information to the responsible parties.

6.3.5 Modification phase

During the system modification phase, any proposed or actual operational system changes beyond the scope of routine maintenance should be reviewed, analysed and, if necessary, tested to determine their impact on operational system security before being implemented in live operation. This includes changes to procedures and policies. Penetration testing of modified controls should be performed to verify their effective operation.

The results of impact analysis and testing should be presented to the Accreditor to determine the need for security re-evaluation. Where modifications are deemed not to have significantly increased the residual risks, perhaps because they have already been assessed as part of a product assurance maintenance process, re-authorization may be given without re-evaluation. However, if the evaluation results have been invalidated, re-evaluation may be required.

The final act of system modification is decommissioning, where a system is closed down and its data archived, destroyed or transferred to other systems. The Accreditor will be required to confirm that the system has been successfully terminated.

6.4 Relationship to other systems

An operational system may interact with other related systems and may form part of a larger whole. The STOE of the evaluated operational system is defined to be that portion of the group of systems that is evaluated, including both IT systems and their operational environment. The remainder is considered to be external operational systems. An operational system may have security objectives that are met by the external operational systems, but these are not analysed or evaluated.

7 Extending ISO/IEC 15408 evaluation concepts to operational systems

7.1 Overview

The purpose of this clause is to document the philosophy that underpins the ISO/IEC 15408 approach to security evaluation and then to extend it to operational systems. ISO/IEC 15408 addresses only technical controls and their related management controls; in operational systems, technical controls and operational controls combine to protect the information and other assets of the organization.

7.2 General philosophy

For many organizations, information is the primary asset and requires protection against the threats of unauthorised release, modification, or destruction. Those assets are protected using a combination of technical controls and supporting operational control infrastructures of personnel, policy, procedures and physical protection measures. The overall ISO/IEC 15408 philosophy is that threats to organizational assets

should be clearly articulated and countered using a combination of technical control and operational control infrastructures. The technical control requirements for addressing threats are included in ISO/IEC 15408-2. Under ISO/IEC 15408, the requirements for the operational controls were considered separately as part of an external accreditation process and therefore were not directly addressed by the security evaluation. This document seeks to formalise those requirements so that they may be assessed as part of the operational system evaluation.

ISO/IEC 15408 conceptually divides security measures into security-related services that must be provided and measures taken to have confidence that those measures are implemented correctly and effectively. In a product evaluation, the security-related services are those functions in the IT implemented to meet the objectives for that piece of technology. In an operational systems context, the procedural and physical contributions to the security can also be assessed. They are similar to IT functionality because they are security capabilities of the operational system that together meet the security objectives. However, they are not normally technology-based and are more suited to assessment during the operational control portion of the operational system life cycle than the development portion. Therefore, they are considered to be separate from functional requirements.

The measures taken to ensure that the security capabilities perform as expected are termed “assurance” in ISO/IEC 15408 and consist of evidence being generated and independent assessment of the suitability of those capabilities. This can be extended to cover the operational controls portion of the operational system through documentation describing the operational controls as implemented.

The process used to develop, implement and maintain both the operational system itself and more specifically the security related services has a considerable influence on the correctness and effectiveness of the security related service and its overall contribution to the total security of the operational system. This influence also contributes to the confidence in the performance of the security related service. Thus the process contributes to the overall assurance of the complex operational system. More specifically the greater the level of capability of the process, the greater the confidence that can be had in the correctness and effectiveness of the security related service and thus the overall assurance provided.

In summary, operational security functional requirements are those non-technical security controls implemented in the operational system contributing to the overall security objectives, while operational security assurance requirements reflect the evidence that those requirements are satisfied.

Evaluation of security in an operational system can therefore be decomposed into a series of steps:

a) The security problem is articulated as a set of risks to be reduced or mitigated, and a set of organizational security policies to be enforced. This requires prior analysis to determine the purpose of the operational system, and risk assessment to determine those risks that must be countered by technical and operational controls. The results of the analysis are recorded in the SST.

b) The security problem is partitioned into a high-level security solution, represented by a set of security objectives. These objectives are recorded in the SST.

c) The security objectives are further refined into security requirements that can be assessed by an independent evaluator. Some security objectives will be allocated to the technical controls and others to operational controls. Some may require both technical and operational controls. For example, controlling unauthorized access to an information asset will often be accomplished both by providing physical security to the facility holding the asset (e.g. locks, guards) and by IT functionality (e.g. user authentication and access control mechanisms). The security requirements are recorded in the SST.

d) A set of activities for the evaluator to follow during the assessment is defined, based on the overall objectives and the overall assurance in the protection measures required. These assurance requirements are recorded in the SST.

e) An independent evaluator assessment determines that the operational system meets its security requirements, based on the requirements documented in the SST.

f) Continuing assessments can also take place to gain confidence that the operational system meets its requirements during operation. These will focus mostly on the operational control portion of the operational system because these controls depend on human behaviour, which is less controllable and consistent than IT behaviour.

g) Periodic re-evaluation of the operational system can assess that the operational system continues to meet its requirements despite changes to the operational system or its environment. This consists of determining what changes have taken place, assessing the security impact of those changes, updating the SST as required, and determining that security has been maintained during this process.

This process is very similar to the ISO/IEC 15408 evaluation process. The typical difference between an operational system evaluation and an ISO/IEC 15408 product evaluation is that in an operational system evaluation the actual operational environment is fully considered, whereas in a product evaluation the operational environment is not defined in detail, it is described purely as assumptions which are not verified during the evaluation.

The primary goal of an operational system evaluation is to gain assurance that the security objectives for the operational system are implemented correctly and effectively. However, evaluation of security controls, whether technical or operational, can never provide absolute assurance that those controls will always function as intended, at all times and in all circumstances. Evaluation produces a pass or fail verdict. Even if evaluation identifies no unacceptable vulnerabilities, there will always be a residual risk that the controls do not perform as intended. This risk can be reduced by adding additional assurance controls or using different assurance measures that give greater confidence. The residual risk of incorrect or ineffective performance of controls can only be identified through continuous monitoring and assessment.

This residual risk must be taken into account when deciding if an operational system can be accredited for live operation.

Environmental factors may result in differing criticality/threat environments for different operational system components. It is possible that some portions of the operational system may require greater assurance while other portions require less assurance. Because risk assessment can establish different levels of acceptability of risk for different portions of the operational system, an operational system can be divided into security domains with different assurance requirements. The risk assessment will determine acceptability of risk for different parts of the operational system and will aid in determining appropriate assurance measures for each part of the operational system.

7.3 Operational system assurance

The ISO/IEC 15408 paradigm for assurance centres on the provision of evidence that the security functions exist and are implemented correctly and effectively. Higher levels of assurance place more detailed requirements on the content and presentation style of the evidence. In addition, higher assurance sometimes requires increasing rigour of analysis of the evidence by both the developer and the evaluator.

An ISO/IEC 15408 product evaluation is conducted in a manner that assumes a generic operational environment in which the product might be employed. The product evaluation focuses on verifying the security capabilities implemented by the product, independent of any specific operational context. The product evaluation utilises various specification, design and test documentation to substantiate the verdict of correctness.

The primary goal of a product evaluation is to gain assurance that the security capabilities of the product are implemented correctly. The basis for correctness is established by the security requirements that are contained in the product's Security Target (ST). The ST includes some traceability on the security problem being solved by the resulting set of security requirements. The security problem stated in the ST is assumed to be based on a threat assessment for the types of environments suitable for deployment of the product. The scope of the product evaluation is limited to the IT security requirements allocated to the product by this threat assessment. In addition, the product evaluation sets bounds for "secure values" for configurable aspects of the product: termed the "evaluated configuration". However, these configurations do not take into account any specific environment as this in unknown at the time of evaluation. Upon completion of the product evaluation, it remains necessary to properly integrate the evaluated product with other products to compose an operational system, and finally, to verify that the operational system provides the desired security properties and behaviour in its operational environment and operational configuration.

Product evaluations generally have the same assurance measures applied across all the security functionality defined. Although it is technically possible to have different security domains in products, this is not usually applied for generic product evaluations.

The evaluation evidence and evaluation reports generated from a product evaluation may be used to support the operational system integration and verification effort.

In principle, there is little difference between the properties of an IT product and an operational system for the purposes of security evaluation. However, operational system evaluation may be significantly more complex than ISO/IEC 15408 product evaluation for a number of reasons:

a) An operational system may comprise many bought-in products and custom IT developments grouped into security domains. The composition of each system security domain may be based upon several factors, such as the technology employed, the functionality provided and the criticality of the assets protected.

b) An operational system may contain multiple instances of the same product (e.g., multiple copies of an operating system provided by the same vendor) or multiple different product instances of the same product type (e.g., multiple firewalls provided by several different vendors).

c) An operational system may have security policies that apply to some security domains while not applying to others.

d) Different residual risks may be acceptable within different domains of an operational system, whereas a product counters specific threats to specific types of asset without consideration of risk.

The main distinction between an ISO/IEC 15408 product evaluation and an operational system evaluation is that an operational system evaluation must fully consider all security controls, including those implemented in the operational environment, which are treated as assumptions in a product evaluation. In general, the type of assurance requirements for technical controls documented in ISO/IEC 15408-3 can be directly applied or easily extended to apply to operational controls. For example, the concept of assessment of design documentation for technical controls becomes assessment of the description of operating procedures for operational controls. The actions of people implementing operational controls can be tested in a similar way to the way that the actions of programs implementing technical controls are tested.

A particular issue concerns assurance of the effectiveness of the controls implementing the SSF. Assurance in this aspect of technical controls is achieved by architectural design techniques such as domain separation, non-interference and non-bypassability of controls. For operational controls, analogous but somewhat different techniques are used, such as separation of duties, inspection and monitoring.

Areas where additional assurance components are needed to handle operational systems are:

a) the overall security architecture and placement of components within the architecture;

b) the configuration of the components that comprise the operational system;

c) the management policies, rules and procedures that govern operation of the operational system;

d) the requirements and rules for interaction with other trusted and untrusted operational systems;

e) the monitoring of the non-IT controls during the operational phase of the system life cycle.

Because of its product focus, ISO/IEC 15408 assumes that a TOE will be developed in a single development environment which is distinct from the intended operational environment. This assumption is unlikely to hold true for most operational systems. Even if the operational system is developed in a separate test environment, the final stage of operational system development will be integration into the operational environment, when the operational control measures are added into the operational system. Some subsystems or components, particularly bought-in products, may also be developed in distinct and different development environments from the main development environment.

This means that some ISO/IEC 15408-3 development environment assurance requirements may not be achievable when developing some operational systems, or their application must be delayed until the system installation life cycle phase. Similarly, assurance in operational controls can only be fully achieved in the operational environment.

7.4 Composite operational systems

Many operational systems are large and complex, offering multiple functions and with a complicated internal structure. Often they are made up of many distinct components and subsystems. Each component may comprise a single function provided by a single product, a single product with multiple functions, or a set of functions implemented by customised software and operational procedures. Some components may be grouped into subsystems, capable of independent execution. Such subsystems might comprise a single client or server constructed from multiple products, multiple servers and/or clients and networks, or heterogeneous clients and/or servers. Some components and subsystems may already be security evaluated; others not.

System owners may have specific time and cost restrictions when deploying new composite operational systems. Thus the processes involved when doing the technical part of the approval to operate (sometimes called site certification as part of an operational system accreditation) need to be adaptable to actual needs.

Typically, composite operational systems:

a) Contain several subsystems or components, with different degrees and types of assurance.

b) Have a well defined control structure. This may be a single operational system “owner” or a defined set of management relationships on the various portions of the operational system.

c) Are built against specific needs for specific operation.

d) Individual components carry a large number of possible configuration options, some of which are inconsistent with the operational system security policies.

e) Enable the operational system owner to implement a different balance of technical controls and operational controls in different parts of the operational system.

The security policy may be different for the different combinations above, except for the rare case in which the operational system has a single function. Logically, all the portions of the operational system under the same set of security policies can be termed a *security domain*. This operational system decomposition of subsystems and components that are governed by the same security policy(s) is then characterized in the security policy in accordance with the appropriate risks to that domain. Functional and assurance security requirements may be identified for each security domain. As such, each security domain will have its own security policy, security problem definition, security objectives, security requirements and security documentation. However, each of these security domains operates within the larger operational system-level set of policies, security problems, objectives, requirements, and documentation. Each security domain may have its own assurance requirements based on the degree of confidence needed in that security domain and its overall contribution to the operational system. The operational system security target will specify the operational system security requirements, which will be a representative compilation of the security domains that comprise the operational system from an operational system context. The security domain concept is illustrated in Figure 2.

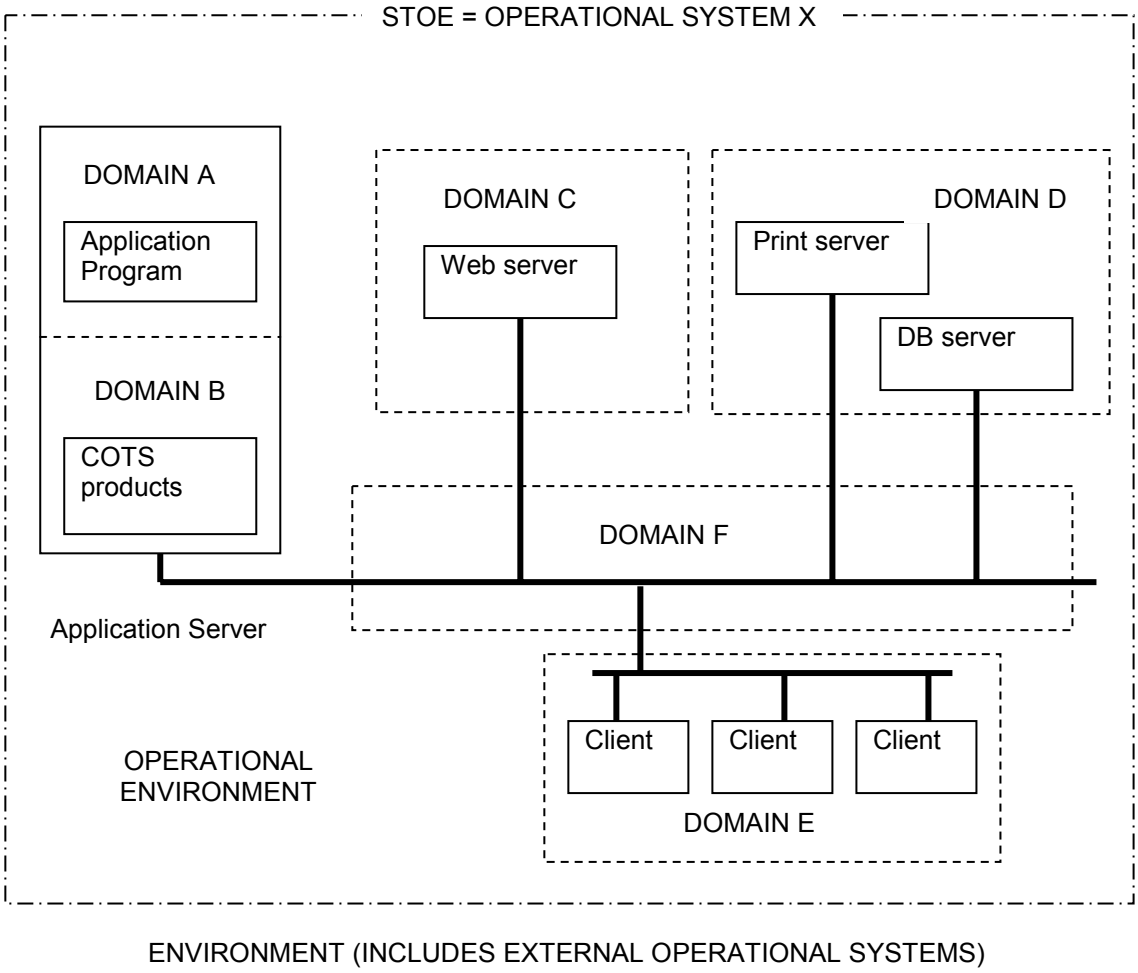

Figure 2 — Example of domains

When constructing a composite operational system there is a need to identify and describe the boundaries of the system, describe the interfaces and dependencies between components of the system, and describe the interfaces and dependencies between components of the system and its environment (e.g. users, external operational systems). All interfaces between components, and between the operational system and its surrounding environment need to be defined. The interface specifications need to cover any security requirements for the interface or for the communications links implementing the interface. In addition, the specifications must identify any trust relations or invariant security properties for the interface.

One benefit of the security domain concept is that it permits different assurance requirements to be applied to different parts of the operational system. Consider a typical server system. It will be constructed from a variety of components, such as application programs, middleware products and base software such as an operating system. The middleware and base software may have been the subject of product evaluations, but may equally well be unevaluated. For non-evaluated products, the vendor may cooperate in providing the evidence needed for evaluation, but also may refuse to make the necessary evidence available. For evaluated products, an Evaluation Technical Report (ETR) may be available to assist in reuse of evaluation results, but access to the ETR may be refused.

Consider the system shown in Figure 3. For security domain A, which is built from proprietary software, it is likely all evaluation evidence required for ISO/IEC 15408 evaluation can be made available. For security domain B, evidence to satisfy some ISO/IEC 15408 criteria might be obtained (e.g. the ADO and AGD classes and ATE_FUN) but some other criteria (e.g. the ADV and AVA classes and ATE_COV/DPT) are unlikely to be achievable as the necessary evidence will have been destroyed or may never have existed. Alternative assurances must be obtained or residual risks accepted.

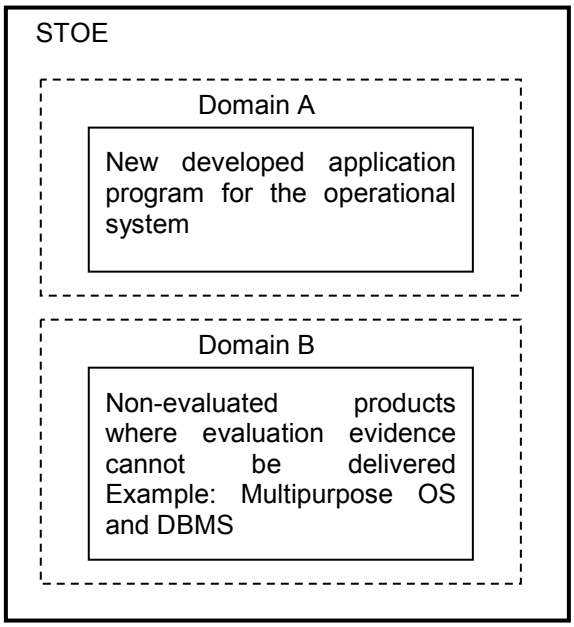

Figure 3 — Heterogeneous system composition

On the other hand, the system shown in Figure 4 is built entirely from components for which evidence required for ISO/IEC 15408 evaluation can be obtained. This can therefore be treated as a single security domain, domain X, with homogenous assurance requirements.

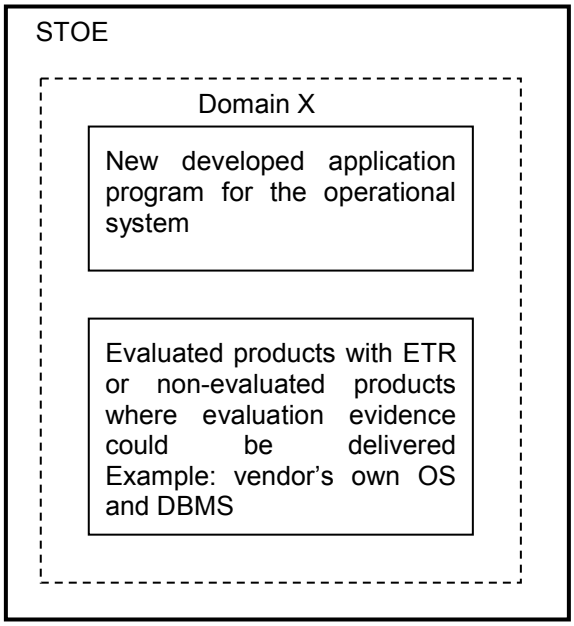

Figure 4 — Homogeneous system composition

In order to achieve its security requirements, one domain within a composite operational system may have dependencies on the security properties of other domains. A domain may offer security services that can be used by other domains through communications or application programming interfaces, or it may enforce security properties on other domains. This needs to be reflected within the SST for the operational system.

Security services and properties that are enforced on or made available to other domains must be identified as such with the statement of security objectives for the domain. Similarly, if a security domain has security objectives that are met by other domains, these must be identified as such within its statement of security objectives.

7.5 Types of security controls

ISO/IEC 15408 mainly specifies technical controls, i.e. security controls that are implemented by the IT components of a system. However, it also needs to specify those management controls and activities that are needed to control and monitor the technical controls.

Operational systems also need to specify operational controls. As for technical controls, operational controls have related management controls and activities which are essential to ensure that they are implemented as specified, do not fall into disuse, and are effective in practice.

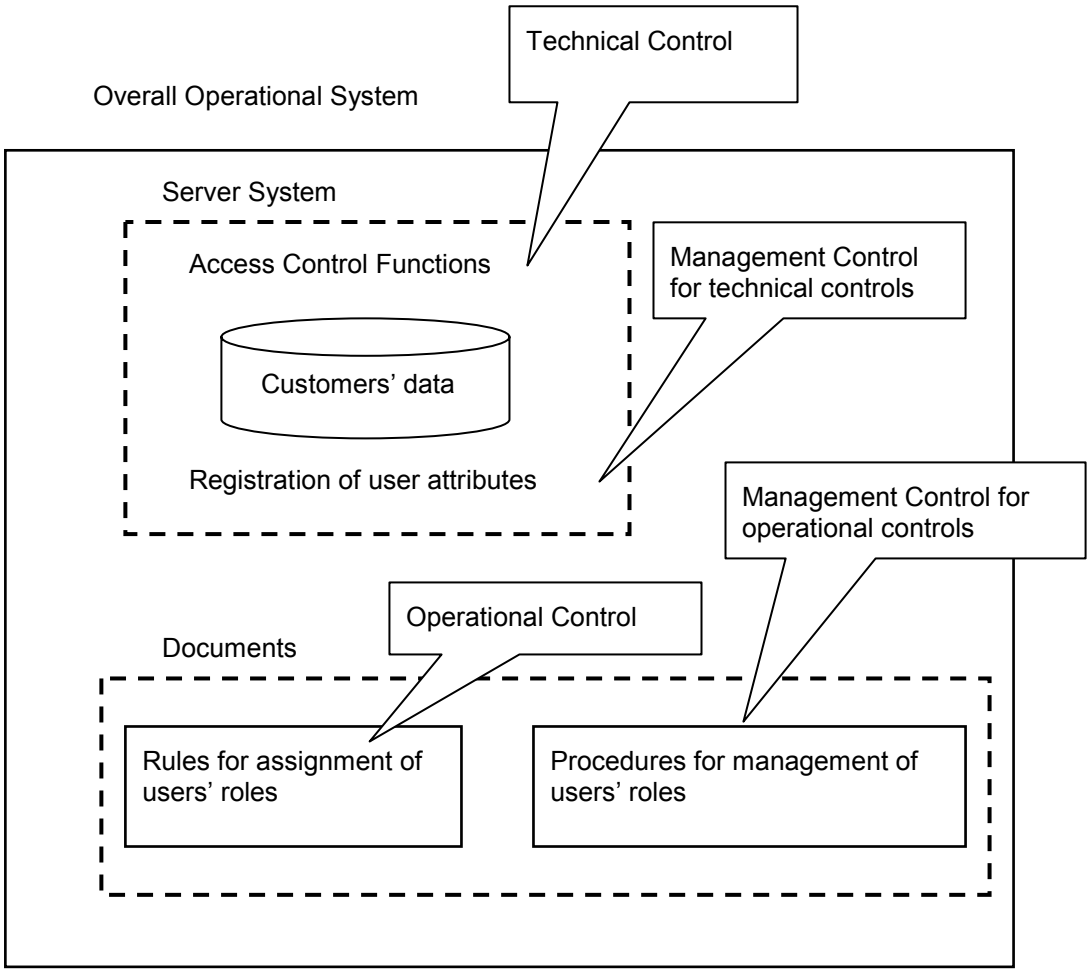

Figure 5 — Example of security controls

Because most operational controls depend on human action which is not necessarily predictable or repeatable, management and monitoring is even more important than for technical controls. In addition, there are controls implemented by system and corporate management designed to ensure the secure operation of the system. These controls could be categorised as either operational controls (since they are part of the operation of the system) or as independent management controls (since they are purely relate to management).

This Technical Report uses the same approach to management controls as in ISO/IEC 15408, namely management controls are always considered to be part of the technical or operational controls that they support.

An example of this is shown in Figure 5 above. In this example, the access control functions implemented by the server are a technical control. The registration of user attributes is a management control that supports the access control functions. However, the rules for assignment of user roles (e.g. to enforce separation of duties) is an operational control. The procedures for management of these users' roles are a management control, but one which supports this operational control.

Operational controls may include rules and procedures as well as physical protection. An example of an operational control that would involve purely management activities is security incident reporting.

For an operational system to be secure, the technical and operational controls (including related management controls) must integrate and work together to provide coverage of all threats. In practice, the contribution to security of the system's technical controls is influenced by and dependent on the operational controls that provide the operational environment. As an example, the value of the system's “IT-asset” to the organization will determine the type of operational controls such as physical protection it is afforded, what personnel will be granted access to it, and under what conditions it will be backed up to support continuing operation. In addition, there may be integration of technical controls and operational controls such as physical protection. For example, physical access operational controls may rely on technical controls for authentication services and operational controls may provide to technical controls information about the physical presence or absence of personnel from a facility.

Many technical controls for operational systems can be expressed directly using ISO/IEC 15408-2 functional components. However, the complexity of operational systems may require additional refinement of components not normally necessary in ISO/IEC 15408 evaluation. Some examples of this are:

a) The administrator might need the capability to ascertain that the operational system configuration is as expected. The requirement for this capability would be a refinement of TSF self-testing (FPT_TST) to be included in the definition of “correct operation of the TOE”.

b) The SST may wish to specifically allocate portions of security functionality to specific components within security domains. This would mean refining “the TSF” to specific portions of the TSF, e.g. “The firewall security domain shall provide a mechanism to…”.

c) It may be necessary to define technical control functions concerning interoperability with other systems, or concerning interoperability between different components or subsystems of the operational system.

Where an ST already exists for the technical controls of an operational system, for example if the controls are provided by a bought-in and evaluated product, the ST can be used as a template for construction of the operational system security requirements. However, since operational system evaluation is risk-based, the threats and assumptions of the product ST and the associated ST rationales will have to be reassessed and possibly amended.

Most operational controls of an operational system address management and operational processes and procedures that are beyond the scope of ISO/IEC 15408 evaluation, and which therefore cannot readily be expressed using ISO/IEC 15408-2 functional components. Additional functional components are needed to handle these requirements, and suitable components are defined in this Technical Report.

7.6 System security functionality

The ISO/IEC 15408 paradigm for security functionality centres around the provision of a TOE which deals with IT security functions only. In an operational system the TOE is generalised into a STOE that includes both the technical and operational control functions.

The system security functionality (SSF) comprises those portions of the STOE (and therefore operational system) relied upon to maintain the security policies for that system. The SSF contains both technical and operational security controls.

When security requirements are defined, the system owner may choose to allocate the requirements to satisfy an objective to either technical security controls, operational security controls or a combination of both.

Three terms are therefore used when defining operational security requirements. When a technical security control is required, the requirement should be expressed in the form “The TSF shall…”. This form is used because ISO/IEC 15408 already uses the term TSF for technical security controls. If an operational security control is required, the requirement should be expressed in the form “The OSF shall…”, indicating the control must be physical, personnel or procedure based. If the implementation could be either technical or operational, or a combination of the two, the requirement should be expressed as “The SSF shall…”.

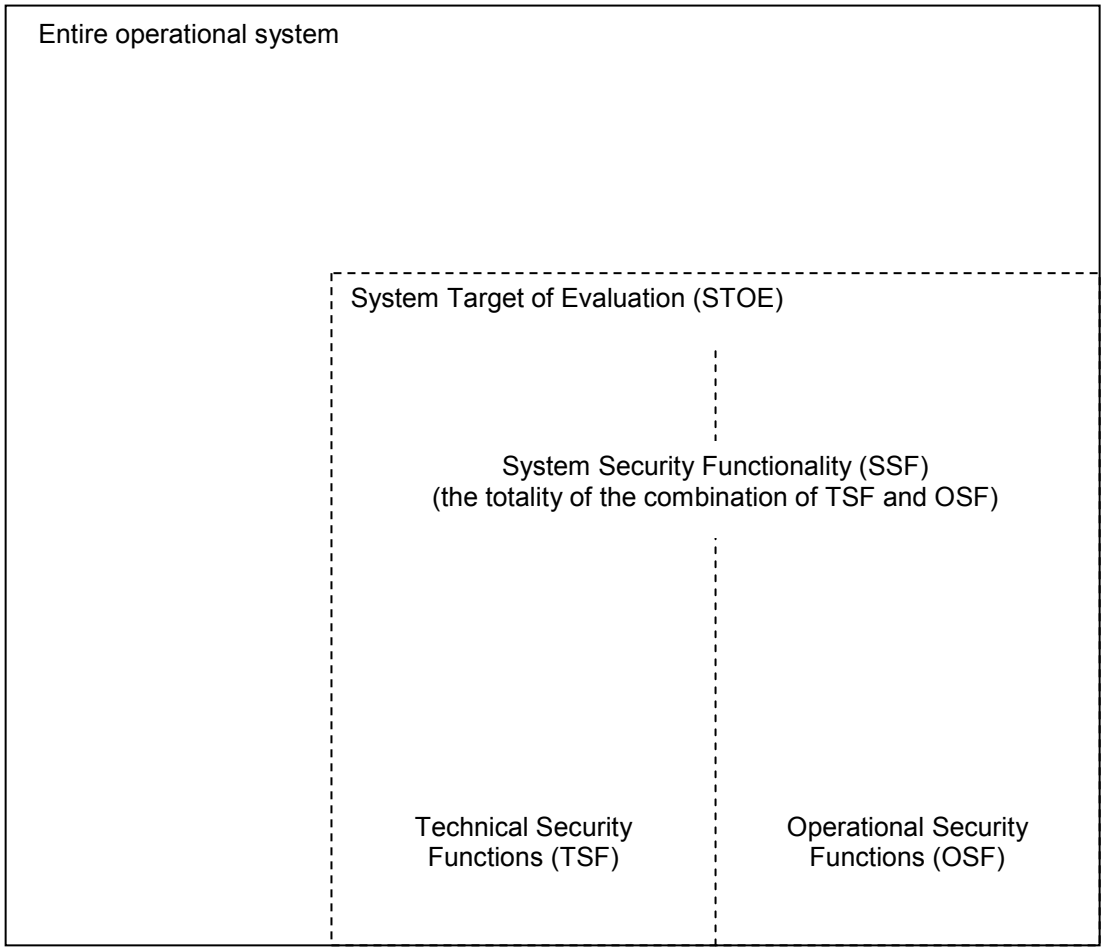

Figure 6 — System security controls

It is important to note that only the security relevant portions of the STOE would be included in the evaluated SSF, and that the STOE need not represent the entire operational system. Figure 6 above provides a pictorial representation of these concepts.

In ISO/IEC 15408 evaluation, technical security functions often have dependencies on aspects of operational security. An example is the ISO/IEC 15408-2 access control element FDP_ACC.1.1:

FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

In ISO/IEC 15408 evaluation, the access control policy and list of subjects, objects and operations would be documented, but otherwise assumed correct. In operational systems evaluation, this policy and list would be evaluated as part of the assessment of data protection and personnel roles and responsibilities (see B.4.2.4, FOA_INF.1.7; and B.2.2.4, FOD_PSN.1.19). In general, rules and procedures required by TSF that must be assumed correct and applicable in ISO/IEC 15408 evaluation will be evaluated as part of an operational systems evaluation.

7.7 Timing of evaluation

Evaluation makes a determination at a given moment of time whether controls meet the requirements placed upon them. This may take place at any time in a product or system's life cycle, but in the case of an ISO/IEC 15408 product evaluation normally takes place once development is complete, but before the product is put into operation.

It is very likely that a technical control that is successfully tested in a development environment will also work in the operational environment. This is much less certain for operational controls. During regular operation, the people in the operational environment may be less trustworthy, less experienced, less competent and/or less motivated than during testing in the development environment. Thus assurance from the development phase in operational controls is much less transferable to the operational environment than assurance in technical controls. It is therefore more likely that initial evaluation will extend into the operational phase, or will take place on a system that already is in operation.

Ideally, an operational system should be re-evaluated following major changes in system capabilities or risks. However, it is also necessary to re-evaluate an operational system periodically to confirm it is still meeting its objectives effectively and to determine whether adjustments are necessary to remain within the risk tolerance required.

In the first case, as for development evaluation, evaluation will provide good evidence that the operational system is capable of meeting its changed objectives but little evidence that such is the case in actual operation. It is left for management to ensure that the operational system security controls are utilised effectively. In the second case, the evaluator can confirm by examination of records of the operation of controls and of security incidents that the controls are meeting their requirements and thus working effectively.

7.8 Use of evaluated products

Where a product has been evaluated, there may be evidence available from the product evaluation that can be reused in operational system evaluation. However, the detailed evidence may not be publicly available. In some instances, this evidence can be obtained directly through an agreement with the product developer or publicly from the scheme's registry for validated products. In others, the relevant detail necessary to determine its applicability to its role in the operational system may not be possible to obtain, and system owner must then determine whether it is acceptable to accept the results without access to the evidence that contributed to those results.

Similarly, it is not necessarily the case that the results of a product evaluation are applicable to the operational system evaluation. Some reasons might be:

a) the configuration of the product during the product evaluation and the configuration of the product when integrated into the operational system may be different.

b) the assurance at which the product was evaluated is inadequate compared to the assurance to which the product is required when integrated as a component in the operational system. In this case, there may be evidence that can be reused but new evidence that will have to be generated as well.

In these instances, the operational system evaluation needs to determine the degree to which the results available can be used and what additional assurance measures may be needed. In the worst case, these components would need to be treated as unevaluated components.

When a product has not completed evaluation, it is unknown how much information might be available to support the operational system evaluation and it is unknown whether any existing product information will be confirmed by the product evaluation. When a product has not been evaluated, information usually required for product evaluation may not be available to support the operational system evaluation. Such considerations would need to be considered in the operational system evaluation.

It is essential that information is available about the security characteristics of the interfaces between products, i.e. which security functions of one product depend on security functions of a different product. It is necessary to confirm in the system evaluation that all products that depend on security functions within other products use those products in a secure manner. Often the necessary information will be documented in the ETR of the other product, but the information may not be presented in a way that is compatible. In this case, it will be necessary to look at other documents such as interface specifications and architectural design documentation as part of system evaluation, and to confirm that the required security properties are present. The same applies where unevaluated products are used.

The variety and maturity of evaluated COTS products that are available for integration into an operational system limits the maximum assurance that can be achieved purely by using evaluated products. In general, it will be impractical to re-evaluate evaluated products at a higher level of assurance, as the additional evidence and developer support are unlikely to be available. If product assurance is not sufficient, it will be necessary to obtain additional assurance from alternative controls or by architectural means, such as adding firewalls or other security-specific architectural components.

Alternatively, an operational system evaluation has the ability to allocate differing levels of assurance across different operational system domains. Where assurance for a particular domain is constrained by the use of evaluated products, the Accreditor can be asked to accept the consequential increased residual risk for that single domain.

7.9 Documentation requirements

In ISO/IEC 15408 product evaluation most documentation requirements are used by the evaluators to confirm that development activities have been performed correctly, and to ensure that users have the necessary information to configure and operate the TOE in a secure manner.

In an operational system, documentation must also be provided that defines the operational controls, so that:

a) the evaluators can confirm that these controls, if properly implemented, will actually satisfy the security objectives placed upon them;

b) checks can be made during the operational phase of the system life cycle that the relevant procedures are being followed, and that both procedural and physical controls are effective.

Documentation must also be provided concerning the security properties of interfaces between different components of the operational system, and between components of the operational system and other systems within its surrounding environment, so that where a component has dependencies on the security properties of another component or system, it can be confirmed by the evaluators that these properties are valid according to the specification of that component or system.

7.10 Testing activities

The testing activities performed as part of operational system evaluation have requirements that are not usually found in ISO/IEC 15408 product evaluation.

Operational system testing assesses the effectiveness of the technical and operational control functions which counter known unacceptable risks and enforce the defined security policies. The effectiveness is determined partly through testing the security functionality of the operational system and partly through conducting penetration testing. Testing is only meaningful after the operational system has been placed into a verified secure configuration. There are two types of configuration: the configuration of the products to interoperate as components of the operational system and the configuration of the products to provide the security behaviour required to enable secure day-to-day operations for the business or mission that the operational system supports. The operational system's technical controls can and should be tested prior to deployment by the system developer/integrator. This testing will provide confidence that the system's technical control functions are working properly and effectively counter the risk to the level intended by the risk assessment. It should also identify any unintended shortcomings and provide the developer with a window to resolve those shortcomings prior to evaluation. The operational controls will then be integrated with the technical control functions at the operational site(s), where the effectiveness of the operational system integrated security controls can be evaluated.

Because operational testing is not part of product evaluation, and ISO/IEC 15408 product evaluation does not require configuration of the product to enforce a specific set of "real-world" operational policies, all products will need to be specifically tested in their operational system configuration as part of the overall operational system testing.

It may also be the case that products or subsystems within an operational system do not interoperate properly. This means the overall operational system testing must investigate and confirm the secure interaction between different components and subsystems.

The internal testing strategy may also be different for different security domains that comprise the operational system, depending on characteristics such as:

a) level of assurance required in the subsystem;

b) level of assurance already established (or not established) in products that comprise the subsystem;

c) architecture chosen and products that comprise the architecture;

d) technology employed;

e) placement of components in the physical environment.

7.11 Configuration management

Operational system evaluation has configuration management requirements that are not usually found in ISO/IEC 15408 product evaluation. ISO/IEC 15408 treats the life cycle of IT products from the perspective of a developer. The life cycle begins with the requirements for the product and then progresses through design, development, evaluation and production. The life cycle only considers operational concerns as it impacts the next version of the product.

Because of this, configuration management is treated primarily as an assurance measure so the evaluator can be sure that the TOE being assessed is the correct version, and can be sure that the developer knows what should be incorporated into the evaluated TOE to be distributed. The configuration management process is not part of the TOE but rather a tool for generating the TOE.

In operational systems it is not only important to know that the correct components are incorporated into the operational system but also that the configuration of the system continues to be known and understood during operation of the operational system. Therefore there may be two different configuration management systems: one for the development environment in which the operational system is produced, and another for the operational environment in which it operates. The first of these is treated as an evaluation assurance and the latter is an operational control capability.

The operational configuration management system exists primarily for the operational system administrators and security managers to be able to establish that the operational system continues to operate in a secure configuration and also to know the impact of updates, removal and insertion of operational system components. Therefore, the operational system needs to have the capability (through either procedural or technological means) to manage the configuration and to report the current configuration. The reporting capability can be used to compare the actual operational system configuration with its intended configuration to facilitate verification that the system security controls are configured correctly, and that security controls have not been changed, due to maintenance action or otherwise and not duly documented. The reporting will also serve to support assurance of any change impact analysis, as a result of continuous monitoring activities. Configuration management therefore becomes a security capability of the operational system. It can be used to provide assurance evidence that the operational controls are correctly and effectively implemented.

8 Relationship to existing security standards

8.1 Overview

This Technical Report provides an extension to ISO/IEC 15408 to permit the evaluation of operational systems. As described in previous clauses, this requires extensions to the model of evaluation found in ISO/IEC 15408 and the definition of additional evaluation criteria.

For the most part, the additional processes, documentation and tasks required for operational system evaluation have been defined by extending analogous concepts within ISO/IEC 15408. The additional evaluation criteria that are required deal primarily with the operational and system integration aspects of information security, and have been derived from existing non-evaluation information security standards. In particular, this Technical Report draws heavily on two specific security best practice standards, ISO/IEC 17799 [4] and NIST SP 800-53 *Recommended Security Controls for Federal Systems* [5]. Given the existence and wide acceptance of these documents, it was considered inappropriate to develop new criteria and criteria structures.

This relationship is shown in Figure 7 following. The SST, system security policy model, risk assessment, vulnerability analysis, guidance documents, procedures, and development design documents will all form part of the documentation provided for the system evaluation and have been generalised from ISO/IEC 15408. The criteria for assessing the operational environment and in particular the operational controls have been drawn from non-evaluation standards and guidelines.

As well as ISO/IEC 17799 and NIST SP 800-53, there are a number of other SC 27 standards, such as ISO/IEC 13335 [1] and ISO/IEC 21827 [6] that have been used as sources. ISO/IEC TR 15443 [3] offers alternative potential approaches with respect to assurance requirements. ISO/IEC TR 15446 [7] suggests guidelines for protection profiles and security target design.

Other relevant documents include NIST SP 800-53A *Guide for Verifying the Effectiveness of Security Controls in Federal Information Systems* [8] and the German *IT Baseline Protection Manual* [9].

Concepts and specific controls have been adapted from all these documents where appropriate. However, evaluation criteria are not intended to define how to design and manage an operational system securely. The purpose of evaluation criteria is to define how to evaluate secure operational systems using evidence provided to evaluators by the system owners, developers, integrators, operators and administrators of the operational system. Evaluation criteria will therefore cover different aspects and have different emphases than the source material from these other standards and guidance documents.

Since the processes, documents and tasks defined within this Technical Report are based on existing ISO/IEC 15408 equivalents, the contributions from other standards and guidelines have been restructured into a format that is an extension of that already used in ISO/IEC 15408.

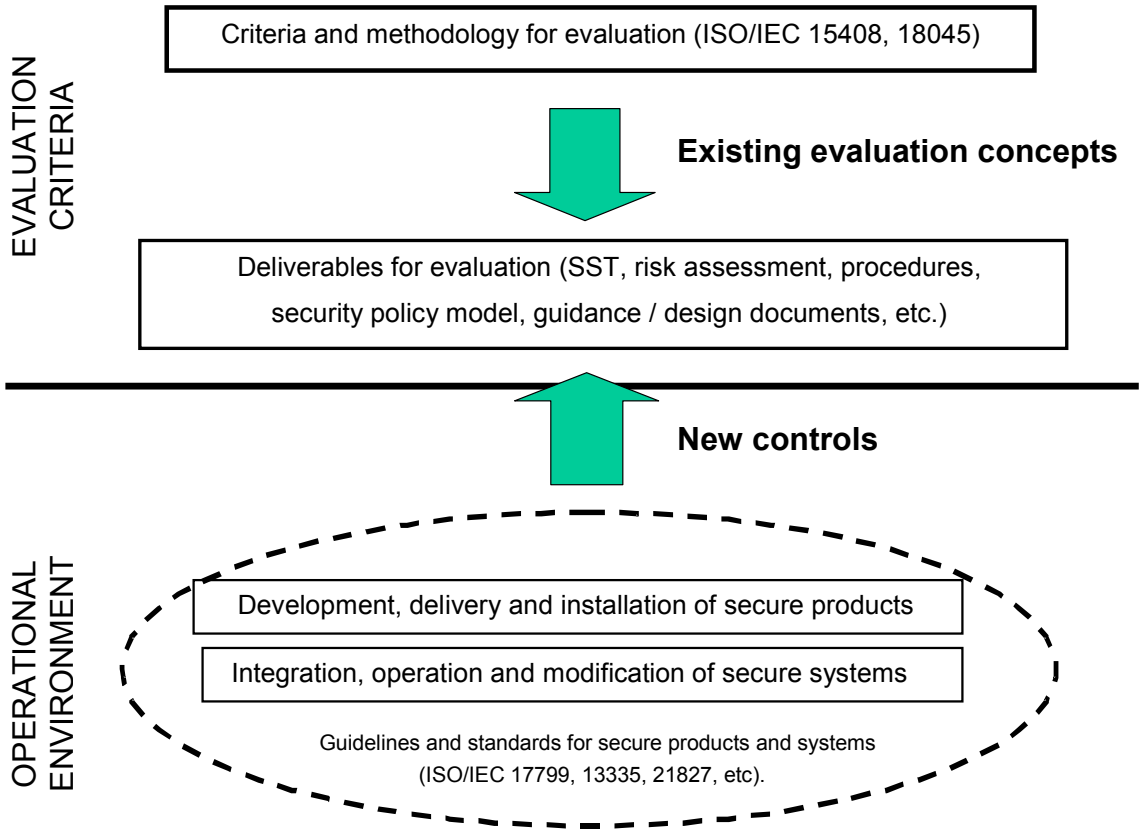

Figure 7 — Relationship between operational environment and evaluation criteria

8.2 Relationship to ISO/IEC 15408

ISO/IEC 15408 has been used as the primary basis and framework for operational system evaluation. It provides the means to specify the requirements for technical controls. For example, it contains criteria for specification of access control policies. ISO/IEC 15408 does not provide the means to specify operational controls, but such controls can be captured within an ISO/IEC 15408-like framework. This then enables the operational system to be assessed using ISO/IEC 15408-like assurance criteria that are verified during the evaluation.

Part 1 of ISO/IEC 15408 defines the concepts of security targets and protection profiles. These requirements specification frameworks serve as the basis for enhanced targets and profiles, System Protection Profiles (SPPs) and System Security Targets (SSTs), that also cover operational controls.

Part 2 of ISO/IEC 15408 defines evaluation criteria for functional requirements. These criteria are directly applicable to the technical controls required for operational systems, and are used as the basis for defining new additional classes, families and components with focus on the operational controls of the operational system within this Technical Report. This Technical Report also captures the “as configured” aspect of the functions and mechanisms within the operational system, and requirements for the policies and procedures that must be implemented in the operational environment by the operational controls.

Part 3 of ISO/IEC 15408 defines criteria for assessing the assurance requirements. These assurance criteria are used as the basis for new assurance classes, families and components with focus on the evaluation activities that must be performed to evaluate the security controls aspects of the operational system as a single integrated unit. This includes the requirements for evidence of the policies and procedures that will be implemented in the operational environment by the operational controls.

8.3 Relationship to non-evaluation standards

ISO/IEC 17799 is a Code of Practice that recommends security controls that should be considered by an organization in order to manage the security of information assets. ISO/IEC 17799 provides recommendations for information security management to initiate, implement and maintain information security within an organization.

ISO/IEC 17799 provides a widely-accepted management framework for the control of operational security. The 2005 edition has been used as the principal source for identifying and specifying aspects of operational security where controls are required, and for formulating specific operational control requirements.

NIST SP 800-53 provides guidelines for selecting and specifying security controls for information systems intended for use in US Government Federal systems. US state, local, and tribal governments as well as private sector organizations comprising the critical infrastructure of the United States are also encouraged to consider the use of its guidelines. It is intended to be replaced by a formal US Federal Standard, FIPS Publication 200, *Minimum Security Controls for Federal Information Systems*. Where appropriate, NIST SP 800-53 draws on ISO/IEC 17799 in the definition of its security controls, but it also covers other areas not directly related to information security management.

NIST SP 800-53 has therefore been used as a secondary principal source for operational controls, particularly in those areas of operational security that are outside the scope of ISO/IEC 17799.

ISO/IEC 13335 also addresses requirements for security controls. However, it deals with controls at too high a level to have been used as a source of specific operational control requirements.

8.4 Relationship to Common Criteria development

The Common Criteria is a technically identical standard to ISO/IEC 15408 published by the Common Criteria Development Board, an association of national schemes for evaluation and certification. Common Criteria Version 2.3 is the equivalent to ISO/IEC 15408:2005, which was used as the baseline for the development of this Technical Report.

The Common Criteria Development Board is currently developing a new version of the Common Criteria, to be called Version 3. Once stable, this version is likely to be used as a major contribution to the future revision of ISO/IEC 15408. The latest draft available at the time of preparation of this Technical Report was Version 3.0 [10]. This version was issued for comment only, i.e. the equivalent of an ISO/IEC Working Draft.

Although Version 3.0 only has comment status, it includes significant developments to evaluation technology based on practical application of the Common Criteria and ISO/IEC 15408. Annex D therefore considers the significant changes incorporated in this new version of the Common Criteria and assesses their potential impact on this Technical Report.

9 Evaluation of operational systems

9.1 Introduction

Operational systems shall be evaluated using the general model of evaluation defined in ISO/IEC 15408-1, with extensions as defined in this clause.

9.2 Evaluation roles and responsibilities

There are three types of activity required for operational system evaluation. These are:

— production of evidence for the evaluation (which includes the risk assessment, SST specification, development and integration, operation, modification);

— evaluation (including certification of evaluation results);

— accreditation.

For each of these activities appropriate personnel shall be assigned, their terms of reference agreed and the necessary tasks performed. These activities and associated roles and responsibilities are listed in Table 1. Each of the different actions required by this Technical Report should readily map to the roles and responsibilities identified in Table 1. Each of the different actions should also map to the SST sections identified in the table.

Table 1 — Roles and Responsibilities for Operational System Evaluation

Activity	Role	Responsibility	SST Sections
Production of the evaluation evidence	Senior Management	Overall responsibility for security. Define acceptable risks. Approve actions of authorized officers	N/A
	Authorized officers of the organization	Assess and accept residual risks.	Security problem definition
	Security agency	Sets organization-wide security policies. Defines mandatory controls to be implemented by all organization systems.	Security problem definition
	System owner	Conducts risk assessment. Defines security problems to be addressed by the system (including objectives, requirements). Prepares any SPP (perhaps as part of a consortium of owners of similar systems) Authorises re-evaluation based on changes to system or its environment. Reviews system status from continuous monitoring reports.	Security problem definition Security objectives Security requirements STOE description
	Developer/ Integrator/System Designer	Production or support of production of SST based on security problem defined by the system owner. Production of development evidence. Assists the system owner to reduce or eliminate vulnerabilities found during evaluation.	STOE description Technical controls Assurance requirements relating to development Architecture and summary specifications
	Operator/ Administrator/ Maintainer	Support of production of SST. Production of operational evidence. Assists the system owner to reduce or eliminate vulnerabilities found during system operation.	Operational controls Assurance requirements related to operation Architecture and summary specifications
Evaluation	Evaluator/ certification agent	Evaluates system based on security requirements articulated in SST, to make determination of system capability to meet its security requirements at that point in time. Provides independent assessment of system security operations throughout system operation Performs re-evaluation, as required, to support changes to the system or its environment. Certifies the evaluation results.	All

Activity	Role	Responsibility	SST Sections
		Provides evaluation and certification reports to system owner, with recommendations, as required, to support system accreditation/authorization	
Accreditation	Accreditor	Authorizes system for use or confirms to the authorized officer that anticipated residual risks are acceptable.	Security problem definition

9.3 Risk assessment and determination of unacceptable risks

Prior to operational systems evaluation, the system owner shall assess the scope of the operational system, determine the assets that need protecting, and, in concert with the authorized officer or designated representative from higher management, determine the level of risk which the organization is willing to accept that each asset of the operational system could be lost, damaged or compromised.

The system owner shall then conduct a risk assessment covering all assets of the operational system. This risk assessment should identify all possible risks to the operational system, including those risks that are countered or eliminated by existing security controls. These existing controls shall be documented as part of the risk assessment, so that they can be included in the SST description of security objectives.

NOTE This Technical Report does not prescribe any particular model or form for risk assessment. Further information about risk assessment of ICT systems can be found in part 1 of ISO/IEC 13335 [1].

Where risks to assets exist that are above the level of risk that the organization is prepared to tolerate, the system owner shall identify a proposed course of action to reduce the risk to an acceptable level. This may take the form of:

— risk acceptance, accepting the increased risk and acknowledging liability for the consequences should the risk be realised;

— risk transfer, transferring the risk or liability for its consequences, to another party;

— risk avoidance, such as by abandoning the activity which causes the risk;

— risk reduction or elimination, reducing the risk to an tolerable level through the implementation of evaluated countermeasures within the operational system to reduce the likelihood and/or the impact of the risk.

Following this analysis, each risk shall then be categorised as acceptable or unacceptable from the point of view of the operational system. Acceptable risks are those which are to be tolerated, accepted, transferred or avoided. Unacceptable risks are those that are to be reduced or eliminated.

Where risks are unacceptable, the system owner in conjunction with the system developer shall identify and specify technical and operational security controls to be implemented as countermeasures. The system owner in conjunction with the system developer shall also identify and specify assurance controls to confirm that the risk that technical or operational security controls fail to meet their security objectives as countermeasures is reduced to a level that the organization is prepared to tolerate.

As part of the operation phase of the system life cycle, the system owner shall periodically review the risk assessment, to determine whether:

— there are changes to business assets;

— there are new risks, or changes to risks to assets;

— the existing countermeasures are still appropriate.

The owner shall then determine if there is a need for the system to be re-evaluated to confirm the adequacy and continued effectiveness of the operational system security controls against the revised risk assessment.

9.4 Security problem definition

The system owner shall define the security problem to be addressed by the operational system and assessed by evaluation. The description of the security problem shall include:

— the results of the risk assessment;

— any organizational security policies that apply to the system.

9.5 Security objectives

The system owner shall prepare a statement of security objectives for the operational system. The security objectives shall provide a concise statement of the intended response to the security problems faced by the operational system.

For operational systems evaluation, two types of security objective must be distinguished:

a) functional security objectives that will be satisfied by technical and operational controls implemented within by the operational system;

b) assurance security objectives that will be satisfied by assurance controls (e.g. verification activities).

In ISO/IEC 15408 evaluation, functional security objectives are normally implemented exclusively by technical controls, since the operational environment is not evaluated, but defined by assumptions within the security problem definition. Within an operational system evaluation, the operational environment is included within the scope of evaluation, and functional objectives may be implemented as technical controls, operational controls, or a combination of the two. Of course, both technical and operational controls may involve associated management controls or actions.

The statement of security objectives shall cover all required controls, including both controls that already exist and those that must be created as part of the implementation of the operational system.

In ISO/IEC 15408 evaluation, the assurance requirements are not normally derived from the security problem. Instead, they are selected axiomatically or by policy decision. Within an operational system, different forms of assurance controls may be required for different components or subsystems, depending on varying types of available development information, or may also depend upon the types of functional controls selected (operational controls may be best assured by different means to technical controls). This means that assurance objectives have to be considered as part of the solution to the security problem.

9.6 Security requirements

9.6.1 Introduction

The system owner shall prepare a set of security requirements for the operational system. The security requirements shall define a set of security controls to be implemented within the operational system (security functional requirements) and shall define the means to assess that the controls are implemented correctly and effectively (security assurance requirements).

9.6.2 Security functional requirements

Technical security controls shall be selected from the functional classes defined within ISO/IEC 15408-2. If no suitable functional components exist within ISO/IEC 15408-2, additional custom components shall be devised and defined in accordance with the procedure defined in ISO/IEC 15408-1:2005, Annex B.

Operational security controls shall be selected from the functional classes defined in Annex B. If no suitable functional components exist within Annex B, additional custom components shall be devised and defined in accordance with the procedure defined in ISO/IEC 15408-1:2005, Annex B.

Table 2 shows a comparison between the functional classes defined in ISO/IEC 15408 and this Technical Report, and their applicability to operational systems evaluation.

Table 2 — Comparison of functional classes

15408:2005	Operational system: 19791	Applicability and coverage
Security audit (FAU)	The same	Applicable
Communication (FCO)		
Cryptography (FCS)		
User data protection (FDP):		
Identification and authentication (FIA)		
Security management (FMT)		
Privacy (FPR)		
Protection of the TOE Security Functions (FPT):		
Resource utilization (FRU)		
TOE access (FTA)		
Trusted path/ channels (FTP)		
	Administration control (FOD)	Policy, Personnel, Risk management, Incident management, Security organization, Service agreement
	IT System control (FOS)	Policy, Configuration, Network security, Monitoring, Personnel control, Operational system assets, Records
	User Assets control (FOA)	Privacy data protection, User assets
	Business control (FOB)	Policy, Continuity
	Facility and Equipment control (FOP)	Mobile, Removable equipment, Remote equipment, System, Facility
	Third Parties control (FOT)	Management
	Management (FOM)	Security parameter, Asset classification, Personnel responsibility, Security organization, Security reporting

9.6.3 Security assurance requirements

Assurance requirements shall be selected from the combination of ISO/IEC 15408-3 and Annex C. If no suitable assurance components exist within ISO/IEC 15408-3 or Annex C, additional custom components shall be devised and defined in accordance with the procedure defined in ISO/IEC 15408-1:2005, Annex B.

Table 3 shows a comparison between the assurance classes defined in ISO/IEC 15408 and this Technical Report, and their applicability to operational systems evaluation.

Table 3 — Comparison of assurance classes

15408:2005	Operational system: 19791	Applicability
APE: Protection Profile evaluation	System Protection Profile evaluation (ASP)	Depend on the difference of SPP
ASE: Security Target evaluation	System Security Target evaluation (ASS)	Depend on the difference of SST
ACM: Configuration management	Operational system configuration management (AOC)	Composition requirements for composed products Configuration management (change, trace, maintain) Confirmation and verification (operation time)
ADO: Delivery and operation	System security installation (ASI)	Awareness training and Communication of SSFs Confirmation and verification (operation time)
ADV: Development	Operational system architecture design and configuration document (ASD)	Interfaces and configuration of components External interfaces Architecture, information flow, access to STOE Mode of operation / transition condition
AGD: Guidance document	Operational system guidance document (AOD)	Rules and procedures for User and Administrator Configuration Confirmation and verification (operation time)
ALC: Life cycle support	Operational system life cycle support (AOL)	The same as security measures for development/ integration environment Confirmation and verification (operation time)
ATE: Tests	Operational system test (AOT)	Functional, coverage and depth test for SSFs Independent testing for SSFs Regression testing at maintenance/modification time
AVA: Vulnerability assessment	Operational system vulnerability analysis (AOV)	Detection of insecure states and their recovery Penetration testing (both operation time and after maintenance/modification)
	Records on operational system (ASO)	Records of SSFs log Management review on SSFs Independent verification of SSFs Confirmation and verification of records,

9.7 The system security target (SST)

The system owner shall record the security problem definition, the security objectives and the security requirements for an operational system in a system security target (SST). The owner shall also obtain and document the other information required to complete the SST as identified in Annex A.

Where the owner of an operational system wishes to define the requirements for an operational system in an implementation independent way, he may first produce or adopt a System Protection Profile (SPP). The mandatory and optional contents of an SPP are defined in Annex A.

The SST serves as the basis for both the documentation of the operational system security capabilities and for the evaluation of those capabilities within the STOE. As such, it provides the evidence and information necessary to perform an evaluation.

An SST differs from an ST due to its focus on both the technical and operational controls of the operational system. An SST may be broken down into several distinct security domains with different functional and assurance controls. However, like an ST, an SST can be evaluated for consistency independently from the STOE.

Subsequently, evaluation of the STOE may identify inconsistencies between the SST and the STOE. The types of discrepancies may include:

a) aspects of the operational system environment as implemented disagree with the operational system environment as specified in the SST;

b) aspects of the operational system security functionality as implemented are different from the operational system security functionality as specified in the SST;

c) aspects of the operational system interfaces and interconnects and their behaviour as implemented disagree with the operational system interfaces as specified in the SST.

The system owner must determine whether the implemented environment, functionality or interface/interconnect is as required, and the description in the SST is wrong, or if the environment, functionality or interface/interconnect should be as specified in the SST. Upon completion of the assessment, appropriate changes must be made. These changes may result in changes to the SST and/or to the operational system. For these reasons, it is impossible for SST evaluation to provide a final verdict as to whether the SST is a correct representation of the desired operational system. Only when STOE evaluation is complete and inconsistencies have been resolved can the SST be confirmed as a correct representation.

Table 4 shows a comparison between the ST defined in ISO/IEC 15408 and the SST defined in this Technical Report, and their applicability to operational systems evaluation.

Table 4 — Comparison of security target elements

15408:2005	Operational system: 19791	Applicability to operational systems
Introduction	Introduction	IT/operational parts of the STOE and interfaces to external operational systems should be defined. Domain organization could be defined.
TOE description		
TOE security environment	Security problems	- Risks should be defined instead of threats. - Assumptions must not be defined, because environments are reality.
Security objectives	Security objectives	Security objectives for IT and operational parts of the STOE and external operational systems should be defined.
IT security requirements	Security requirements	Functional requirements for IT parts of the STOE Operational requirements for operational parts of the STOE Assurance requirements should be defined.
TOE summary specification	STOE summary specification	Functional, operational and assurance specifications should be described.
PP claims	Compliance claim	Compliance claim for SPPs, PPs, and/or STs could be defined.
	Domain introduction	IT/operational parts of the domain should be defined.
	Domain security problem definition	Risks and OSPs should be defined
	Domain security objectives	Security objectives for IT and operational parts of the domain should be defined.
	Domain security requirements	Functional requirements for IT and operational parts of the domain should be defined. - Assurance requirements for the domain should be defined.

15408:2005	Operational system: 19791	Applicability to operational systems
	Domain summary specification	Functional, operational and assurance specifications for the domain should be described.
	Domain compliance claim	Compliance claim for SPPs, PPs, and/or STs for the domain could be defined

9.8 Periodic reassessment

The system owner shall specify controls to ensure that the results of evaluation of an operational system remain valid during system operation.

This can be done in two ways:

— Management controls can be specified to check periodically that the configuration of the technical controls has been maintained and the operational control measures are being faithfully implemented. To do this, a set of processes and procedures must be created to manage the security impact of changes as they occur in the operational environment. It must include regression testing of all system changes, to ensure that system controls are not modified or disabled.

— An evaluator can periodically re-evaluate the operational system STOE, concentrating on whether the combination of technical and operational control measures needs adjustment to meet the changing security requirements of the organization, and to confirm that operational processes and procedures are being applied effectively.

Annex A
(normative)

Operational system Protection Profiles and Security Targets

A.1 Specification of System Security Targets

A.1.1 Overview

This section defines the concept and content of a System Security Target (SST).

Table A.1 — Summary of ST and SST differences

	"Product" ST	SST
Specification framework	Single "box" focus	Focus increase to address larger and more complex grouping of system components, which can be decomposed into security domains.
Security objectives	IT specific; and no direct mapping of security objectives to assurance requirements.	Specific objectives traced back to specific assurance requirements. Operational controls (physical, procedural and policy) relationships and their contribution to system security documented to and assurance measures selected.
Environment documentation	Minimally addressed outside of risk assessment arena and seen as assumptions	Should be clearly defined and documented. No assumptions.
Risk Assessment	Cites non-IT, especially procedures, as assumptions and product compliance related	Identifies risks as "known" and operational controls may call for evaluation as to their adequacy in integrated system environment
TOE description	IT focused	Defines technical and operational controls environment, their interfaces, and their inter-relationships.
Compliance claims	Strictly IT functionality	Can re-allocate functionality between system components (e.g., technical and operational controls).
System architecture	Based on "stand-alone" product	Typically broken into distinct security domains with different controls. Addresses interactions between domains and between domains and the surrounding environment

The SST provides a specification for the implemented security capabilities of an operational system as it is employed in a specific operational context to counter assessed risks and/or enforce stated organizational security policies to achieve an acceptable level of residual risk. The operational system is composed of an integrated combination of technical and operational control functions. The SST describes the requirements and behaviour of the functions that implement the security objectives through a combination of technology-based and operational-based mechanisms. Additionally, the SST describes the measures that provide assurance in terms of the ability of the operational system to meets its functional objectives while operating at an acceptable level of residual risk.

The SST serves as a suitable basis for conducting the operational system evaluation. The SST must therefore provide a description of the operational system that is:

a) Sufficiently complete. Each risk is sufficiently countered and each organizational security policy is sufficiently enforced by the combination of technical and operational control functions.

b) An appropriate and necessary solution for the stated problem. The combination of technical and operational control functions is effective in countering the unacceptable risks and enforcing the organizational security policies, and the assurance measures provide sufficient assurance that the security functions are correctly and effectively implemented.

c) An accurate instantiation of any SPP, PP or ST to which it claims compliance, either in whole or in part.

The concept and structure of an SST are based on expansion of the ISO/IEC 15408 concept and structure for Security Targets (STs). Table A.1 above provides a summary of the conceptual differences between a ST and SST.

A.1.2 SST contents

An SST shall conform to the content requirements described in this annex. An SST should be presented as a user-oriented document that minimises reference to other material that might not be readily available to the SST user. The rationale may be supplied separately, if that is appropriate.

An SST shall include the following:

a) a common part applicable to the whole STOE;

b) domain parts, one for each security domain defined within the STOE, and describing the unique aspects of that domain.

The common part shall contain:

a) SST introduction;

b) conformance claims;

c) security problem definition;

d) security objectives;

e) extended components definition;

f) security requirements;

g) STOE summary specification.

For each security domain forming part of the operational system, the following shall be included:

a) security domain introduction;

b) security domain conformance claims;

c) security domain security problem definition;

d) security domain security objectives;

e) security domain security requirements;

f) security domain summary specification.

Certain sections of the SST may be empty if there is no relevant information to be provided. Conformance claims only appears if the SST claims compliance with one or more SPPs, PPs or STs. Certain subsections of the security domain information are optional. They need only be specified if security domains have unique security problems, objectives or requirements that do not apply to the STOE as a whole.

The specifications presented in this section are derived in part from the ST specifications contained in ISO/IEC 15408-1:2005, Annex A, and in part from additional SST requirements defined in this Technical Report.

A.1.3 SST introduction

The SST introduction shall identify the SST and STOE, and provide an STOE overview, an STOE description and domain organization. It shall contain document management and overview information as follows:

a) The **SST/STOE identification** shall provide the labelling and descriptive information necessary to control and identify both the SST and the STOE to which it refers.

b) The **STOE overview** shall summarize the objectives of the STOE in narrative form. The overview should be sufficiently detailed for a potential user of the SST to determine whether the SST is of interest.

c) The **STOE description** shall outline the functions and boundaries of the STOE in narrative form.

d) The **domain organization specification** shall describe the breakdown of the STOE into domains with unique security requirements.

There is no prescribed content or layout for the STOE overview, but it should specify the purpose or mission of the operational system, an overview of the system in the context of its operational environment and descriptions of the system from the point of business, management and technical architecture. It should define the relationship between the STOE and external operational systems, and the interfaces between the STOE and those systems.

There is no prescribed content or layout for the STOE description, but it should describe the scope and boundaries of the STOE from both logical and physical points of view. It should also describe the organisation and location where the STOE was developed, including any unique characteristics for individual domains e.g. domains based on commercial products.

Operational systems are composed of one or more security domains. Each security domain includes some components and may have its own security assurance requirements. The domain organization specification shall document the organization of the security domains, their domain boundaries and their interfaces in detail.

In the best possible case, the STOE will be composed of components that fully define the operational system as a closed entity whereby there are no interfaces to external operational systems that are not included in the evaluation. From a practical standpoint, this best case is sometimes not possible and it is necessary to define a clear partition between those parts of the operational system that will undergo evaluation as an integrated unit and those parts that are outside the scope of the evaluation. The components that are outside the scope of the evaluation are treated as part of external operational systems.

The operational system concept has basis in the interfaces that exist between the components of the operational system. Without interfaces, there is no operational system. Therefore, the interfaces are critical to the operational system definition and equally critical to the ability of the operational system to enforce a security policy across its interfaces. The domain organization specification will provide an overview of the various components of the operational system, including how they interface. The details of the interfaces are left to interface specifications for the design and integration of the operational system. However, the domain organization specification should identify all security properties of individual domains that are enforced on other domains, and also all security services offered by individual domains that are available to other domains.

A.1.4 Conformance claims

This section is only applicable if the SST claims compliance with one or more SPPs, PPs, STs or security requirement packages. The conformance claims section provides evidence that the SST is an acceptable instantiation of any SPP, PP, ST or requirements package for which compliance is being claimed. A conformance claims rationale shall demonstrate consistency between the SST security objectives and requirements and those of any SPP, PP, ST or requirements package to which conformance is claimed.

The focus of the compliance claim is on “equivalence” in terms of meeting the base set of criteria stated in the SPPs, PPs, STs or requirements packages. The SST may be a functional superset of a package or profile but it shall not be a sub-set.

A primary difference between operational system and product compliance claims is that for the operational system it may be appropriate to reallocate functionality between the technical and operational control portions of the operational system because it is all considered part of the STOE. In a product evaluation, allocation of IT functionality to the non-IT environment changes the entire concept of the product and defeats the purpose of the product evaluation activity.

A.1.5 Security problem definition

A.1.5.1 Overview

The SST security problem definition section shall provide a coherent, consistent and sufficiently complete definition of the security problems that the operational system is intended to address. The security problems are stated in terms of the risks that will be countered by the operational system and the organizational security policies that support and govern the use of the operational system to reduce operational system risk to an acceptable level.

The security problem definition shall define:

a) all risks that are applicable to the STOE;

b) all organizational security policies that apply to the STOE.

In this section, security problems that are concerns to the whole STOE should be defined. It is possible that different security domains of the STOE will execute in different operational environments, and as a result, there may be different or unique risks or policies that must be addressed independently by different security domains of the operational system. For each security domain, additional security problems that are concerns to that domain only should be defined.

Recognising that this section is preceded by the STOE introduction, it is important that any material presented in this section of the SST is consistent with the information provided in the STOE introduction.

A.1.5.2 Risk identification

In this section all risks that are applicable to the STOE shall be described, based upon a risk assessment of the operational system. Each risk shall be categorised as acceptable or unacceptable, i.e. requiring reduction or elimination through technical or operational controls within the STOE. Those risks that are accepted must still be identified, since acceptability of risks may change over time.

The list of risks shall include risks relating to the development of the operational system. The description of each risk shall be sufficiently detailed to identify the assets that can be damaged or compromised, the threats and vulnerabilities applicable to each asset and the impact of successful attack. Threats should be characterised in terms of the associated threat agents and their potential adverse actions on assets. The risk assessment should identify all possible risks to the operational system, including those risks that are countered or eliminated by existing security controls.

NOTE Threat agents can include natural events such as accidents, as well as human beings and computer processes acting on their behalf.

With time, additional risks may be identified or the consequences of a security breach may change. Risk assessment must be repeated through the system life cycle, and, if necessary, the SST updated and the operational system re-evaluated.

In this section, those risks should be identified and categorised that relate to operation of the system as a whole, for example risks relating to employees or business assets. Some risks, for example risks relating to application processing, may only apply to a particular security domain and should be therefore be identified and analysed for that domain only.

A.1.5.3 Organizational security policies (OSPs)

In operational systems, the OSP scope is expanded to include the life-cycle management and operations issues that are not addressed during an ISO/IEC 15408 evaluation. These policies include:

a) governing laws, mandates and directives;

b) business continuity;

c) inter-organizational use agreements (i.e. Inter-Service Agreement (ISA) or Memorandum of Understanding (MOU)).

A.1.6 Security objectives

The security objectives contained in the SST security objectives section shall provide a coherent, consistent and sufficiently complete high level description of the security solution based upon the definition of unacceptable risks and organizational security policies in the security problem definition section. The high level description is made in terms of functional security objectives that are subsequently allocated to the technical and operational controls of the operational system or to other operational systems that interface to the operational system. A security objectives rationale shall demonstrate that the stated security objectives are traceable to all of the aspects identified in the SST security problem definition and are suitable to cover them. It should provide complete traceability between the stated security objectives and all aspects of the statement of the security problem, and it should provide sufficient information to determine whether the security objectives sufficiently counter the stated unacceptable risks and enforce the stated organizational security policies.

There is another type of security objective which governs the verification activities to generate and analyse the evidence and to observe or test the implementation to determine that it is implemented in accordance with the requirements. This type of security objective is typically not justified in ISO/IEC 15408 evaluation (i.e. specific objectives are not traced back to specific assurance requirements). As a result, there is little, if any substance in product PP/ST documents that justifies the assurance measures selected. However, for an operational system, a clear statement of assurance objectives is needed, derived from assurance aspects of the security problem, in order to justify assurance measures that will apply to the whole of the operational system. These measures may apply either to the development environment of the TOE or its operation.

The statement of security objectives must cover all required controls, including both controls that already exist and those that must be created as part of the implementation of the operational system.

Security objectives selected to implement one aspect of the security problem may also provide solutions or partial solutions in other areas. In particular, security objectives may address risks which have been accepted following risk assessment, i.e. categorised as tolerable, acceptable, transferable or to be avoided. Such linkages must still be identified and recorded, as acceptability of risks may change over time.

The security objectives provide the highest level statement of the strategy and philosophy for countering the defined risks and for enforcing the defined organizational security policies. In operational systems, it is critical that security objectives are precise. Precision is required both in terms of how the objectives trace back and cover statements made in the security problem definition and also in terms of how the security objectives allocate the solution to the operational system components and physical processes.

The security objectives must be considered against the stated risks and organizational security policies in finer detail when compared to how they are considered in the product sense. This is because of the impact the environment has in regards to the operational system evaluation and the detailed knowledge about the environment that must be captured in the security objectives.

In addition, operational system security objectives must ensure there is a balance achieved in the management of overall residual risk.

It is possible that different security domains of the operational system will support and execute in different operational environments. For example, the capability for the operational system to monitor internal network traffic might be configured as “off” whereas the capability for the operational system to monitor incoming traffic to the internal network is configured as “on”. As a result, there may be different or unique security objectives for different security domains. There may also be additional assurance objectives for particular security domains to meet unique assurance requirements that apply only to those domains.

A.1.7 Extended components definition

In some cases, suitable components to describe the security requirements will not exist within ISO/IEC 15408 or this Technical Report. In such cases, new components shall be defined within this section of the SST. These extended components can then be used to define additional functional and additional assurance requirements.

A.1.8 Security requirements

The security requirements section shall provide a complete and consistent set of security requirements for the STOE. This includes both the operational system security functional requirements and the operational system security assurance requirements. It applies to both the technical and operational control measures to be provided to meet the operational system security objectives. These requirements must provide an adequate basis for the development of security processes, procedures, mechanisms and services that may be configured to enforce defined policies and to counter identified risks. A security requirements rationale shall demonstrate that the set of security requirements is suitable to meet and traceable to all SST security objectives.

In some cases, the security requirements for an operational system may be stated without justification; i.e. they are not derived from security objectives which are themselves derived from definitions of security problems. In these cases, the objectives and security problem definition sections of the SST may be omitted.

The security requirements section shall describe all system security functions and systems security assurances required by the operational system in terms of completed security components.

It is possible that different security domains of the operational system will support and execute in different operational environments. As a result, there may be different or unique security functional requirements for each security domain, required to meet the unique security objectives of that domain. Similarly, security assurance requirements need not be applied across all operational system components to the same depth and breadth. It is necessary to allocate the appropriate level and types of assurance to the various security domains defined in the SST.

A.1.9 STOE summary specification

The STOE summary specification shall provide a coherent, consistent and sufficiently complete high-level description of the security mechanisms, services, interfaces, operational controls and assurance measures, and demonstrate that these satisfy the specified operational system security requirements. A STOE summary specification rationale shall show that the STOE security functions and assurance measures are suitable to meet the STOE security requirements.

It is necessary that enough of the operational system architecture is defined in the SST for a reader to understand the solution being provided to meet the requirements. Details on the definition of subsystems, interfaces and interconnections, and the allocation of functional requirements to the various subsystems that

comprise the operational system should be left for design documentation to follow. The architecture and summary specification should address interactions between security domains and interactions between domains and their environment.

A.1.10 Security domain information

The security domain information section of the SST shall provide information concerning each security domain forming part of the complete operational system. It shall provide an accurate and correct identification of each security domain and any domain-specific security information that is required.

If there is only one security domain within the STOE, it need not be explicitly named or identified, and this section should be omitted.

The security domain information for each security domain shall contain the following:

a) The **security domain introduction** shall provide the labelling and descriptive information necessary to control and identify the security domain and the STOE to which it refers, and summarize the domain in narrative form. The overview should be sufficiently detailed to understand the business functions of the security domain and its security requirements.

b) The **security domain conformance claims** shall define any conformance claims that are unique to the domain. If the security domain has no unique conformance claims, this section may be omitted.

c) The **security domain security problem definition** shall define any security problems that are unique to the domain. This shall include policies and risks that are unique to the domain. If the security domain has no unique security problems, this section may be omitted.

d) The **security domain security objectives** shall define any security objectives that are unique to the domain. This shall include any security objectives that are available to other domains, or which are implemented by other domains. If the security domain has no unique security objectives, this section may be omitted.

e) The **security domain security requirements** shall define any security requirements that are unique to the domain. If the security domain has no unique security requirements, this section may be omitted.

f) The **security domain summary specification** shall define any mechanisms, services, interfaces, operational controls and assurance measures that are unique to the domain. If the security domain has no unique mechanisms, services, interfaces, operational controls or assurance measures, this section may be omitted.

A.2 Specification of System Protection Profiles

A.2.1 Overview

This section defines the concept and content of a System Protection Profile (SPP).

Table A.2 — Summary of PP and SPP differences

	Product PP	System PP
Specification Framework	Single “box” focus	Focus increase to address larger and more complex grouping of products, which comprise operational system, with physically dispersed distribution, and integrated security controls
Focus	More narrow and IT specific	Broader, flexible and incorporates security controls aspects of system security – flexible to account for varying business cases
Operational Controls (Physical, OSPs, Personnel..)	Minimally addressed outside of risk assessment arena – assumes environment contributions	Addresses as full partner with technical controls as contributor to system security to meet operational needs
Risk Assessment	Cites non-IT, especially procedures, as assumptions and product compliance related	Identifies risks as “known” and operational controls may call for evaluation as to their adequacy in integrated system environment
TOE description	Narrow and IT focused	Broader incorporating internal interfaces as well as interfaces to “external/remote” systems, subsystems, and components.

The SPP conceptually serves the same function as an ISO/IEC 15408 Protection Profile - the SPP presents a characterisation of an acceptable solution to a security problem. The SPP, however, has to handle the integration of technical and operational security controls and may need to integrate multiple components or subsystems with differing security policies and/or operational environments.

An SPP must be capable of presenting options and conditional solutions. An example would be in the definition of security objectives. There may be both technical control and operational control solutions that address a specific risk and which would be equally acceptable from the operation and cost points of view. An SPP might offer several applicable and reasonable solutions for an SST author to select one of them.

Equally, an SPP must be capable of mandating certain common security controls. For example, there may be a policy within an organization that certain operational controls will be applied to all information systems within that organization.

Finally, the SPP specification framework must have sufficient flexibility to enable an operational system evaluated based on an SPP to be reused as an evaluated component of a larger system.

An SPP can also be used as part of the procurement specification for acquiring an operational system. To be suitable for this purpose, the SPP must provide a description of the operational system security capabilities that is:

a) Sufficiently complete. Each risk is sufficiently countered and each organizational security policy is sufficiently enforced by the mandated combination of technical and operational control functions (or a chosen option where the SPP permits alternatives).

b) An appropriate and necessary solution for the stated security problem. The combinations of technical and operational control functions are effective in countering the unacceptable risks and enforcing the organizational security policies, and the assurance measures provide sufficient assurance that the security functions are correctly and effectively implemented.

c) An accurate instantiation of any SPP or PP to which it claims compliance, either in whole or in part.

The concept and structure of an SPP are based on expansion of the ISO/IEC 15408 concept and structure for Protection Profiles (PPs). Table A.2 above provides a summary of the differences between a PP and SPP.

A.2.2 SPP contents

An SPP shall conform to the content requirements described in this annex. An SPP should be presented as a user-oriented document that minimises reference to other material that might not be readily available to the SPP user. The rationale may be supplied separately, if that is appropriate.

An SPP shall include the following:

a) a common part applicable to the whole STOE;

b) domain parts, one for each security domain defined within the STOE, and describing the unique aspects of that domain.

The common part shall contain:

a) SPP introduction;

b) conformance claims;

c) security problem definition;

d) security objectives;

e) extended components definition;

f) security requirements.

For each security domain forming part of operational systems meeting the SPP, the following shall be included:

a) security domain introduction;

b) security domain conformance claims;

c) security domain security problem definition;

d) security domain security objectives;

e) security domain security requirements.

Certain sections of the SPP may be empty if there is no relevant information to be provided. Certain subsections of the security domain information are optional. They need only be specified if security domains have unique security problems, objectives or requirements that do not apply to the STOE as a whole.

The specifications presented in this section are derived in part from the PP specifications contained in ISO/IEC 15408-1, Annex B, and in part from additional SPP requirements defined in this Technical Report.

A.2.3 SPP introduction

The SPP introduction shall identify the SPP and provide an STOE overview and domain organization. It shall contain document management and overview information as follows:

a) The **SPP identification** shall provide the labelling and descriptive information necessary to control and identify the SPP.

b) The **STOE overview** shall summarize the STOE represented by the SPP in narrative form. The overview should be sufficiently detailed for a potential user of the SPP to determine whether the SPP is of interest. The overview should also be usable as a stand alone abstract for use in SPP catalogues and registers.

c) The **domain organization specification** shall describe the breakdown of the STOE into domains with unique security requirements.

There is no prescribed content or layout for the STOE overview, but it should specify the purpose or mission of the operational system, an overview of the system in the context of its operational environment and descriptions of the system from the point of business, management and technical architecture. It should define the relationship between the STOE and external operational systems, and the interfaces between the STOE and those systems.

Operational systems are composed of one or more security domains. Each security domain includes some components and may have its own security assurance requirements. The domain organization specification shall document the organization of the security domains, their domain boundaries and their interfaces in detail.

In the best possible case, the STOE will be composed of components that fully define the operational system as a closed entity whereby there are no interfaces to external operational systems that are not included in the evaluation. From a practical standpoint, this best case is sometimes not possible and it is necessary to define a clear partition between those parts of the operational system that will undergo evaluation as an integrated unit and those parts that are outside the scope of the evaluation. The components that are outside the scope of the evaluation are treated as part of external operational systems.

The operational system concept has basis in the interfaces that exist between the components of the operational system. Without interfaces, there is no operational system. Therefore, the interfaces are critical to the operational system definition and equally critical to the ability of the operational system to enforce a security policy across its interfaces. The domain organization specification will provide an overview of the various components of the operational system, including how they interface. The details of the interfaces are left to interface specifications for the design and integration of the operational system. However, the domain organization specification should identify all security properties of individual domains that are to be enforced on other domains, and also all security services offered by individual domains that are to be available to other domains.

A.2.4 Conformance claims

This section is only applicable if the SPP claims compliance with one or more SPPs, PPs or security requirements packages. The conformance claims section provides evidence that the SPP is an acceptable instantiation of any SPP, PP or requirements package for which compliance is being claimed. A conformance claims rationale shall demonstrate consistency between the SPP security objectives and requirements and those of any SPP, PP or requirements package to which conformance is claimed.

The focus of the compliance claim is on “equivalence” in terms of meeting the base set of criteria stated in the SPPs or PPs. The SPP may be a functional superset of a package or profile but it shall not be a sub-set.

A primary difference between operational system and product compliance claims is that for the operational system it may be appropriate to reallocate functionality between the technical and operational control portions of the operational system because it is all considered part of the STOE. In a product evaluation, allocation of IT functionality to the non-IT environment changes the entire concept of the product and defeats the purpose of the product evaluation activity.

A.2.5 Security problem definition

A.2.5.1 Overview

The SPP security problem definition section shall provide a coherent, consistent and sufficiently complete definition of the security problems that operational systems meeting the requirements of the SPP are intended to address. The security problems are stated in terms of the risks that will be countered by the operational system and the organizational security policies that support and govern the use of the operational systems meeting the requirements of the SPP to reduce operational system risk to an acceptable level.

The security problem definition shall define:

a) all risks that are applicable to the STOE;

b) all organizational security policies that apply to the STOE.

In this section, security problems that are concerns to the whole of operational systems meeting the requirements of the SPP should be defined. It is possible that different security domains of operational systems meeting the SPP will execute in different environments, and as a result, there may be different or unique policies or risks that must be addressed independently by different security domains of the operational system. For each security domain, additional security problems that are concerns to that security domain only should be defined.

If risk assessment of an actual operational system indicates that there are risks not identified in the SPP, then it will be necessary to modify the system boundaries to eliminate those risks, or introduce the additional risks into the SST risk identification section.

Recognising that this section is preceded by the STOE introduction, it is important that any material presented in this section of the SPP is consistent with the information provided in the STOE introduction.

A.2.5.2 Risk identification

In this section all risks that are applicable to the STOE shall be described, based upon a risk assessment of the operational system or types of operational system covered by the SPP. Each risk shall be categorised as acceptable or unacceptable, i.e. requiring reduction or elimination through technical or operational controls within the STOE. Those risks that are accepted must still be identified, since acceptability of risks may change over time.

The list of risks shall include risks relating to the development of the operational system. The description of each risk shall be sufficiently detailed to identify the assets or types of asset that can be damaged or compromised, the threats and vulnerabilities applicable to each asset or type of asset and the impact of successful attack. Threats should be characterised in terms of the associated threat agents and their potential adverse actions on assets. The risk assessment should identify all possible risks to operational systems meeting the requirements of the SPP.

NOTE Threat agents can include natural events such as accidents, as well as human beings and computer processes acting on their behalf.

With time, additional risks may be identified or the consequences of a security breach may change. Risk assessment must be repeated through the system life cycle, and, if necessary, the SPP updated and the operational system re-evaluated.

In this section, those risks should be identified and categorised that relate to operation of systems meeting the requirements of the SPP as a whole, for example risks relating to employees or business assets. Some risks, for example risks relating to application processing, may only apply to a particular security domain and should be therefore be identified and analysed for that domain only.

A.2.5.3 Organizational security policies (OSPs)

In operational systems, the OSP scope is expanded to include the life-cycle management and operations issues that are not addressed during an ISO/IEC 15408 evaluation. These policies include:

a) governing laws, mandates and directives;

b) business continuity;

c) Inter-organizational use agreements (i.e. Inter-Service Agreement (ISA) or Memorandum of Understanding (MOU)).

A.2.6 Security objectives

The security objectives contained in the SPP security objectives section shall provide a coherent, consistent and sufficiently complete high level description of the security solution based upon the definition of unacceptable risks and organizational security policies in the security problem definition section. The high level description is made in terms of functional security objectives that are subsequently allocated to the technical and operational controls of operational systems meeting the requirements of the SPP or to other operational systems that interface to that operational system. A security objectives rationale shall demonstrate that the stated security objectives are traceable to all of the aspects identified in the SPP security problem definition and are suitable to cover them. It should provide complete traceability between the stated security objectives and all aspects of the statement of the security problem, and it should provide sufficient information to determine whether the security objectives sufficiently counter the stated unacceptable risks and enforce the stated organizational security policies.

There is another type of security objective which governs the verification activities to generate and analyse the evidence and to observe or test the implementation to determine that it is implemented in accordance with the requirements. This type of security objective is typically not justified in ISO/IEC 15408 evaluation (i.e. specific objectives are not traced back to specific assurance requirements). As a result, there is little, if any substance in product PP/ST documents that justifies the assurance measures selected. However, for an operational system, a clear statement of assurance objectives is needed, derived from assurance aspects of the security problem, in order to justify assurance measures that will apply to the whole of the operational system. These measures may apply either to the development environment of the TOE or its operation.

The statement of security objectives must cover all required controls, including both controls that are assumed to already exist and those that must be created as part of the implementation of the operational system.

Security objectives selected to implement one aspect of the security problem may also provide solutions or partial solutions in other areas. In particular, security objectives may address risks which have been accepted following risk assessment, i.e. categorised as tolerable, acceptable, transferable or to be avoided. Such linkages must still be identified and recorded, as acceptability of risks may change over time.

The security objectives provide the highest level statement of the strategy and philosophy for countering the defined risks and for enforcing the defined organizational security policies. In operational systems, it is critical that security objectives are precise. Precision is required both in terms of how the objectives trace back and cover statements made in the security problem definition and also in terms of how the security objectives allocate the solution to the operational system components and physical processes.

The security objectives must be considered against the stated risks and organizational security policies in finer detail when compared to how they are considered in the product sense. This is because of the impact the environment has in regards to the operational system evaluation and the detailed knowledge about the environment that must be captured in the security objectives.

In addition, operational system security objectives must ensure there is a balance achieved in the management of overall residual risk.

It is possible that different security domains of operational systems meeting the requirements of the SPP will support and execute in different operational environments. For example, the capability for the operational

systems to monitor internal network traffic might be configured as “off” whereas the capability for the operational systems to monitor incoming traffic to the internal network is configured as “on”. As a result, there may be different or unique security objectives for different security domains. There may also be additional assurance objectives for particular security domains to meet unique assurance requirements that apply only to those domains.

A.2.7 Extended components definition

In some cases, suitable components to describe the security requirements will not exist within ISO/IEC 15408 or this Technical Report. In such cases, new components shall be defined within this section of the SPP. These extended components can then be used to define additional functional and additional assurance requirements.

A.2.8 Security requirements

The security requirements section shall provide a complete and consistent set of security requirements for the STOE. This includes both the operational system security functional requirements and the operational system security assurance requirements. It applies to both the technical and operational control measures to be provided to meet the operational system security objectives. These requirements must provide an adequate basis for the development of security processes, procedures, mechanisms and services that may be configured to enforce defined policies and to counter identified risks. A security requirements rationale shall demonstrate that the set of security requirements is suitable to meet and traceable to all SPP security objectives.

In some cases, the security requirements in an SPP may be stated without justification; i.e. they are not derived from security objectives which are themselves derived from definitions of security problems. In these cases, the objectives and security problem definition sections of the SPP may be omitted.

The security requirements section shall describe all system security functions and systems security assurances required by the operational systems meeting the requirements of the SPP in terms of completed security components.

It is possible that different security domains of operational systems meeting the requirements of the SPP will support and execute in different operational environments. As a result, there may be different or unique security functional requirements for each security domain, required to meet the unique security objectives of that domain. Similarly, security assurance requirements need not be applied across all operational system components to the same depth and breadth. It is necessary to allocate the appropriate level and types of assurance to the various security domains defined in the SPP.

A.2.9 Security domain information

The security domain information section of the SPP shall provide information concerning each security domain mandated by the SPP. It shall provide an accurate and correct identification of each security domain and any domain-specific security information that is required.

If the SPP does not mandate more than one security domain, it need not be explicitly named or identified, and this section should be omitted. Note that architectural considerations may mean that an SST based on the SPP introduces additional security domains in order to permit a cost effective solution to the security problems.

The security domain information for each mandated security domain shall contain the following:

a) The **security domain introduction** shall provide the labelling and descriptive information necessary to control and identify the security domain and the STOE to which it refers, and summarize the domain in narrative form. The overview should be sufficiently detailed to understand the business functions of the security domain and its security requirements.

b) The **security domain conformance claims** shall define any conformance claims that are unique to the domain. If the security domain has no unique conformance claims, this section may be omitted.

c) The **security domain security problem definition** shall define any security problems that are unique to the domain. This shall include policies and risks that are unique to the domain. If the security domain has no unique security problems, this section may be omitted.

d) The **security domain security objectives** shall define any security objectives that are unique to the domain. This shall include any security objectives that are available to other domains, or which are implemented by other domains. If the security domain has no unique security objectives, this section may be omitted.

e) The **security domain security requirements** shall define any security requirements that are unique to the domain. If the security domain has no unique security requirements, this section may be omitted.

Annex B
(normative)

Operational system functional control requirements

B.1 Introduction

This annex defines operational system control functional requirements covering the management and procedural aspects of a STOE. The requirements described herein work in conjunction with technical functional requirements taken from ISO/IEC 15408-2 to meet the security objectives of an STOE. ISO/IEC 15408-2 is used as the basis for the structure for these components.

Operational control functional requirements are categorised by considering subjects, functional areas and actions. The subject is the direct target for controls, such as business data, information processing facilities or IT systems. The functional area is the target for the defined operations, such as policy, risk management or recording. Each functional area constructs a family within a class. The action is an operation in a defined functional area, and constructs a component within that family. Elements are the concrete definition of rule and procedures for controls.

Seven new classes of operational controls are defined in this annex. They are:

a) Administration (FOD), which specifies provides operational control requirements relating to system administration;

b) IT systems (FOS), which specifies operational control requirements supporting the use of IT systems and equipment;

c) User assets (FOA), which specifies operational control requirements relating to the control of user assets;

d) Business (FOB), which specifies operational control requirements relating to business processes and functions;

e) Facility and Equipment (FOP), which specifies operational control measures relating to business equipment, facilities and premises;

f) Third party (FOT), which specifies the operational control measures to relationships with third parties;

g) Management (FOM), which specifies the operational control measures relating to management activities.

The families within these classes are shown in Table B.1.

Table B.1 — Operational control functional families

Class	Family
Administration (FOD)	Policy administration (FOD_POL)
	Personnel administration (FOD_PSN)
	Risk management administration (FOD_RSM)
	Incident management administration (FOD_INC)
	Security organization administration (FOD_ORG)
	Service agreements administration (FOD_SER)
IT Systems (FOS)	Policy for IT systems (FOS_POL)
	Configuration of IT systems (FOS_CNF)
	Network security of IT systems (FOS_NET)
	Monitoring of IT systems (FOS_MON)
	Personnel control of IT systems (FOS_PSN)
	Operational system assets of IT systems (FOS_OAS)
	Records for IT systems (FOS_RCD)
User Assets (FOA)	Privacy data protection (FOA_PRO)
	User assets information protection (FOA_INF)
Business (FOB)	Business policies (FOB_POL)
	Business continuity (FOB_BCN)
Facility and Equipment (FOP)	Mobile equipment (FOP_MOB)
	Removable equipment (FOP_RMM)
	Remote equipment (FOP_RMT)
	System equipment (FOP_SYS)
	Facility management (FOP _MNG)
Third Parties (FOT)	Third party commitments (FOT_COM)
	Third party management (FOT_MNG)
Management (FOM)	Management of security parameters (FOM_PRM)
	Management of asset classification (FOM_CLS)
	Management of personnel security responsibilities (FOM_PSN)
	Management of security organization (FOM_ORG)
	Management of security reporting (FOM_INC)

The dependencies between components of these families are shown in Table B.2 following. Each of the components that is a dependency of some functional component is allocated a column. Each functional component with dependencies is allocated a row. The value in the table cell indicates whether the column label component is directly required (indicated by a cross “X”), or indirectly required (indicated by a dash “-”) by the row label component.

Table B.2 — Operational control dependencies

	FOD_PSN.1	FOD_PSN.3	FOD_PSN.5	FOD_RSM.1	FOD_ORG.1	FOD_ORG.2	FOS_POL.1	FOS_POL.4	FOS_NET.1	FOA_POL.3	FOM_PRM.2	FOM_INC.1
FOD_INC.1						X						X
FOS_SER.1									X			
FOS_POL.1											X	
FOS_PSN.1	X	X									X	
FOS_OAS.1							X				-	
FOA_INF.1							X				-	
FOB_POL.1							X				-	
FOB_BCN.1				X								
FOP_MNG.1			X									
FOT_MNG.1		X										
FOM_PRM.1								X				
FOM_PSN.1										X		
FOM_ORG.1					X							
FOM_ORG.2						X						

Some requirements for operational controls will always be implemented as operational requirements and are therefore defined as OSF. Others could be either operational or technical and are therefore described as SSF.

There are four presentational differences to ISO/IEC 15408-2. There are no hierarchical operational control components, so that subheading is omitted throughout. All management activities are handled by explicit components, and thus no management activities subheadings are needed. The audit subheading has been changed to records, which better expresses the necessary evidence gathering process for operational controls. The assignment permitted operation has been used more flexibly than as used in ISO/IEC 15408-2. Identification of documents that describe associated policy, procedures, rules, security requirements and other controls may be specified as an assignment.

B.2 Class FOD: Administration

This class provides operational control requirements for administration of an operational system.

B.2.1 Policy administration (FOD_POL)

B.2.1.1 Family behaviour

This family defines operational system security policies for administration. It includes specification of security policy, management forum, management review and management controls for security violation.

B.2.1.2 Component levelling

FOD_POL.1 Security policy. Management controls, goals and objects of the security policy, management review and management controls for security violation are defined.

FOD_POL.2 Data protection and privacy policy. Data protection and privacy policy is defined.

B.2.1.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOD_POL.1**: Description of management commitment, security policy, management review and management controls for security violation with concrete actions and specifications.

For **FOD_POL.2**: Description of data protection and privacy policy.

B.2.1.4 FOD_POL.1 Security policy

Dependencies: no dependencies.

FOD_POL.1.1 The OSF shall define [assignment: *management commitment*] that management will actively support security within the organization through clear direction, demonstrated commitment, explicit assignment and acknowledgment of information security responsibilities.

FOD_POL.1.2 The OSF shall define [assignment: *information security policy*] including goals, objectives, scope, compliance with legislative, contractual and standards requirements, risk assessment and risk management, security education, training, and awareness requirements, business continuity management, consequences of information security policy violations and the organization's responsibilities and its approach to managing information security.

FOD_POL.1.3 The OSF shall define [assignment: *formal procedures*] for management reviews that include the information on results of independent reviews, results of previous management reviews, changes that could effect the organization's approach to managing information security, recommendations provided by relevant authorities, trends related to threats and vulnerabilities, and reported security incidents as the input.

FOD_POL.1.4 The OSF shall define [assignment: *personnel policy*] providing a means for personnel to receive retraining of violation of operational controls.

FOD_POL.1.5 The OSF shall define [assignment: *security requirements*] for means to communicate the action upon the violation of operational controls that will take place before personnel are given access to system assets.

FOD_POL.1.6 The OSF shall define [assignment: *personnel policy*] providing a means to impose sanctions such as monetary fine, removal of privileges, suspension or other penalty upon the violation of operational controls.

FOD_POL.1.7 The OSF shall define [assignment: *security requirements*] that remove, limitation, or other actions to the violator from access to system assets until criteria for reinstatement.

FOD_POL.1.8 The OSF shall define [assignment: *personnel policy*] by providing a means to terminate personnel upon violation of rules and procedures, as permitted by law.

FOD_POL.1.9 The OSF shall define [assignment: *security requirements*] for all relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements and to be kept up to date for each information system and the organization.

FOD_POL.1.10 The OSF shall define [assignment: *information security policy*] that an appropriate set of procedures for information labelling and handling is developed and implemented in accordance with the classification scheme adopted by the organization.

FOD_POL.1.11 The OSF shall define [assignment: i*nformation security policy*] that the organization's approach to managing information security and its implementation (i.e. control objectives controls, policies, processes, and procedures for information security) is reviewed independently at planned intervals, or when significant changes to the security implementation occur.

FOD_POL.1.12 The OSF shall define [assignment: *information security policy*] that all identified security requirements are addressed before giving users access to the organization's information or assets.

FOD_POL.1.13 The OSF shall define [assignment: *information security policy*] that an information security policy document is approved by management, and published and communicated to all employees and relevant external parties.

B.2.1.5 FOD_POL.2 Data protection and privacy policy

Dependencies: no dependencies.

FOD_POL.2.1 The OSF shall develop and implement [assignment: *data protection and privacy policy*].

B.2.2 Personnel administration (FOD_PSN)

B.2.2.1 Family behaviour

This family defines security administration of personnel in the operational system. It includes specification of personnel roles and responsibilities, disciplinary action, contents of personnel agreement, management of user identification, control of assets and information security awareness, education, and training.

B.2.2.2 Component levelling

FOD_PSN.1 Personnel roles and responsibilities. Management responsibilities, responsibilities for performing the exit process, legal responsibilities and security controls for the personnel working in the secure area are defined. A formal disciplinary process is defined. Term and conditions of the assignment contract and rules to sign a confidentiality or non-disclosure agreement are defined. Rules to supervise or clear visitors are defined. Rules to take aware of precise scope of the permitted access are defined. Rules regarding acceptable use and return of organizational assets are defined.

FOD_PSN.2 Information security awareness, education and training. Requirements for information security awareness, education, and training are defined.

B.2.2.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOD_PSN.1**: Description of management responsibilities, responsibilities for performing the exit process, legal responsibilities, security controls for the personnel working in the secure area, a formal disciplinary process with concrete actions, specifications and records on conducting the disciplinary action, term and conditions of the assignment contract, rules to sign a confidentiality or non-disclosure agreement, rules on conducting the user identification, rules to take aware of precise scope of the permitted access and rules regarding acceptable use and return of organizational assets with concrete actions and specifications and records on conducting the control.

For **FOD_PSN.2**: The records of conducting information security awareness, education and training.

B.2.2.4 FOD_PSN.1 Personnel roles and responsibilities

Dependencies: FOD_POL.1 Security Policy

FOD_RSM.1 Risk management within the organization

FOD_PSN.1.1 The OSF shall define and document [assignment: *roles and responsibilities*] of employees, contractors and third party user in accordance with the organization's information security policy.

FOD_PSN.1.2 The OSF shall define [assignment: *responsibilities*] for performing employment termination or change of employment.

FOD_PSN.1.3 The OSF shall define [assignment: *security requirements*] for on-going security requirements, legal responsibilities, confidentiality agreement and the terms and conditions continuing for defined period after the end of the employee's, contractor's or third party user's assignment for the communication of exit responsibilities.

FOD_PSN.1.4 The OSF shall define [assignment: *security requirements*] for personnel working in secure areas.

FOD_PSN.1.5 The OSF shall define [assignment: *security requirements*] that access rights of all employees and contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

FOD_PSN.1.6 The OSF shall define [assignment: security *requirements*] on all candidates for staff, contractors and third party users in accordance with relevant laws, regulations.

FOD_PSN.1.7 The OSF shall define [assignment: *procedures*] developed and followed when collecting and presenting evidence for the purposes of disciplinary action handled within an organization.

FOD_PSN.1.8 The OSF shall define [assignment: security *requirements*] on a formal disciplinary process for employees, contractors and third party users who have committed a security breach.

FOD_PSN.1.9 The OSF shall define [assignment: *security requirements*] on term and conditions of the assignment contract which state: the employee's, contractor's and third party user's legal responsibilities and rights, responsibilities for the classification and management of organizational data handed by the employee's, contractor's and third party user's, responsibilities of the employer for the handling of personal information, including personal information created as a result of, or in the course of, assignment with the organization, responsibilities which are extended outside the organization's premises and outside normal working hours and actions to be taken if the employee, contractor or third party user disregards the employer's security requirements to all people employed by the organization, new employees, contractors and third party users. The responsibilities contained within the term and conditions of employment shall continue for a defined period after the end of the assignment.

FOD_PSN.1.10 The OSF shall define [assignment: *rules*] that as part of their contractual obligation, employees, contractors and third party users agree and sign their and the organization's responsibilities for information security.

FOD_PSN.1.11 The OSF shall define [assignment: *rules*] to sign a confidentiality or non-disclosure agreement as part of their initial term and conditions of employment prior to being given access to information processing facilities and that requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information are identified and regularly reviewed.

FOD_PSN.1.12 The OSF shall define [assignment: *security requirements*] for confidentiality agreement when there are changes to terms of assignment or contract, particularly when employees are due to leave the organization, or contracts are due to end.

FOD_PSN.1.13 The OSF shall define [assignment: *rules*] that all personnel to wear some form of visible identification.

FOD_PSN.1.14 The OSF shall define [assignment: *rules*] not to access to organizational facilities except that which is authorized.

FOD_PSN.1.15 The OSF shall define [assignment: *rules*] concerning acceptable use of information and organizational assets.

NOTE Organizational assets include previously issued software, corporate documents, mobile computing devices, credit cards, access cards, software, manuals and information stored on electronic media.

FOD_PSN.1.16 The OSF shall define [assignment: *rules*] that all employees and contractors and third party users to return all the organization's assets in their possession upon termination of their employment, contract or agreement.

FOD_PSN.1.17 The OSF shall define [assignment: *rules*] that all employees and contractors and third party users not to take organizational assets off-site without authorization.

FOD_PSN.1.18 The OSF shall define [assignment: *rules*] that duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

FOD_PSN.1.19 The OSF shall define [assignment: *security requirements*] on a formal disciplinary process for employees who have committed a security breach.

B.2.2.5 FOD_PSN.2 Information security awareness, education and training

Dependencies: no dependencies.

FOD_PSN.2.1 The OSF shall define and document [assignment: *security requirements*] that all employees of the organization, contractors and third party users receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

FOD_PSN.2.2 The OSF shall define and document [assignment: *security requirements*] that awareness training should commence with a formal induction process designed to introduce the organization's security policies and expectations before access to information or services is granted.

FOD_PSN.2.3 The OSF shall define and document [assignment: *security requirements*] that ongoing training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities, use of software packages and information on the disciplinary process.

B.2.3 Risk management administration (FOD_RSM)

B.2.3.1 Family behaviour

This family defines risk management for administration. It includes risk management to the organization and to related third parties.

B.2.3.2 Component levelling

FOD_RSM.1 Risk management within the organization. The procedures for risk management to the organization are defined.

FOD_RSM.2 Risk management relating to third party access. The procedures for risk management of access by third parties are defined.

B.2.3.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOD_RSM.1**: Description of the risk management to the organization with concrete actions and specifications and records on conducting the risk management.

For **FOD_RSM.2**: Description of the risk management of third party access with concrete actions and specifications and records on conducting the risk management.

B.2.3.4 FOD_RSM.1 Risk management within the organization

Dependencies: no dependencies.

FOD_RSM.1.1 The OSF shall define [assignment: *procedures*] for risk management to lists of organizational information and information processing facilities, including home workers and other remote or mobile users.

FOD_RSM.1.2 The OSF shall define [assignment: *security requirements*] for conducting of risk management to the operational system with business process..

FOD_RSM.1.3 The OSF shall define [assignment: *security requirements*] that timely information about technical vulnerabilities of information systems being used is obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

B.2.3.5 FOD_RSM.2 Risk management relating to third party access

Dependencies: no dependencies.

FOD_RSM.2.1 The OSF shall define [assignment: *procedures*] for risk management of lists of organizational information and information processing facilities which third parties will access with the consideration of lists of controls employed by the third parties, legal and regulatory requirements the third party should take into account and contractual obligations the organization and the third party needs to take into account of.

FOD_RSM.2.2 The OSF shall define [assignment: *procedures*] that the risks to the organization's information and information processing facilities from business processes involving external parties are identified and appropriate controls implemented before granting access.

B.2.4 Incident management administration (FOD_INC)

B.2.4.1 Family behaviour

This family defines incident management for administration. It includes specification of incident management.

B.2.4.2 Component levelling

FOD_INC.1 Security incidents. A formal security incident reporting procedure, incident management procedures and action to recovery are defined.

B.2.4.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOD_INC.1**: Description of a formal security incident reporting procedure, incident management procedures and action to recovery with concrete actions and specifications and records on security incident reports and their management.

B.2.4.4 FOD_INC.1 Security incidents

Dependencies: FOM_INC.1 Reporting detected security problems

FOD_ORG.2 Management forum responsibilities.

FOD_INC.1.1 The OSF shall define [assignment: *procedures*] for a formal security incident reporting together with an incident response procedure, setting out the action to be taken on receipt of an incident report.

FOD_INC.1.2 The OSF shall specify [assignment: *security requirements*] for a point of contact where everybody wanting to report an incident can turn to.

FOD_INC.1.3 The OSF shall define [assignment: *procedures*] for incident management to handle potential types of security incident, including system failures and loss of service, viruses and other forms of malicious code, denial of service, errors resulting from incomplete or inaccurate business data, breaches of confidentiality, integrity, accountability, authenticity, reliability or privacy, and misuse of information systems.

FOD_INC.1.4 The OSF shall define [assignment: *security requirements*] on action to recovery from security breaches and correct system failures.

FOD_INC.1.5 The OSF shall define [assignment: *security requirements*] on recording of faults reported by users regarding problems with information processing or communications systems.

FOD_INC.1.6 The OSF shall define [assignment: *procedures*] that security incidents should be reported through appropriate management channels as quickly as possible.

FOD_INC.1.7 The OSF shall define [assignment: *rules*] to ensure that that all employees, contractors and third party users of information systems and services are aware of the procedure for reporting security incidents and the point of contact.

FOD_INC.1.8 The OSF shall define [assignment: *rules*] that all employees, contractors and third party users of information systems and services are required to note and report any observed or suspected security weaknesses in systems or services.

FOD_INC.1.9 The OSF shall define [assignment: *responsibilities and procedures*] for management to ensure a quick, effective, and orderly response to information security incidents.

FOD_INC.1.10 The OSF shall define [assignment: *mechanisms*] in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

FOD_INC.1.11 The OSF shall define [assignment: *security requirements*] that where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence is collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

B.2.5 Security organization administration (FOD_ORG)

B.2.5.1 Family behaviour

This family defines administration of the security organization. It includes specification of a management forum.

B.2.5.2 Component levelling

FOD_ORG.1 Security coordination responsibilities. The responsibilities for security coordination are defined.

FOD_ORG.2 Management forum responsibilities. The responsibilities of a management forum are defined.

B.2.5.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOD_ORG.1**: Description of the responsibilities for security coordination with concrete actions and specifications.

For **FOD_ORG.2**: Description of the responsibilities of the management forum with concrete actions and specifications.

B.2.5.4 FOD_ORG.1 Security coordination responsibilities

Dependencies: no dependencies.

FOD_ORG.1.1 The OSF shall define [assignment: *responsibilities*] that information security activities are co-ordinated by representatives from different parts of the organization with relevant roles and job functions.

FOD_ORG.1.2 The OSF shall define [assignment: *security requirements*] that appropriate contacts with relevant authorities are maintained.

FOD_ORG.1.3 The OSF shall define [assignment: *security requirements*] that appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.

B.2.5.5 FOD_ORG.2 Management forum responsibilities

Dependencies: no dependencies.

FOD_ORG.2.1 The OSF shall define [assignment: *responsibilities*] for a management forum dealing with security issues.

FOD_ORG.2.2 The OSF shall define [assignment: *requirements*] for the management forum to ensure that security activities are executed in compliance with the information security policy; approve methodologies and processes for information security, risk assessment, information classification, identify threat changes and exposure of information and information processing facilities to threats and assess the adequacy and co-ordinate the implementation of information security controls.

B.2.6 Service agreements administration (FOD_SER)

B.2.6.1 Family behaviour

This family defines service agreements on security administration. It includes specification of network services security requirements.

B.2.6.2 Component levelling

FOD_SER.1 Network services agreements. Security features, service levels and management requirements of network services are defined.

B.2.6.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOD_SER.1**: Description of security features, service levels and management requirements of network services with concrete actions and specifications.

B.2.6.4 FOD_SER.1 Network services agreements

Dependencies: FOS_NET.1 Network services.

FOD_SER.1.1 The OSF shall define [assignment: *security requirements*] on identification of security features, service levels and management requirements of all network services and inclusion of them in a network service agreement.

FOD_SER.1.2 The OSF shall define [assignment: *security requirements*] on the ability of the network service provider to manage agreed services in a secure way and agreement of the right to audit.

FOD_SER.1.3 The OSF shall establish [assignment: *agreements*] for the exchange of information and software between the organization and external parties.

B.3 Class FOS: IT systems

This class provides operational control requirements for IT systems in the operational system.

B.3.1 Policy for IT systems (FOS_POL)

B.3.1.1 Family behaviour

This family defines security policies for IT systems in the operational system. It includes specification of security requirements, change control, malicious code control and cryptography.

B.3.1.2 Component levelling

FOS_POL.1 Security requirements. Update management procedures and identification of changes, change control and introduction of changed system are defined.

FOS_POL.2 Malicious code policy. Management procedures to deal with malicious code are defined.

FOS_POL.3 Mobile code policy. Management procedures to deal with mobile code are defined.

FOS_POL.4 Cryptography policy. Procedures for use of cryptographic techniques, management procedures for cryptographic keys are defined.

FOS_POL.5 Public systems. Protection procedures for publicly available system are defined.

B.3.1.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOS_POL.1**: Description of the security requirements and change controls with concrete actions and specifications and records on conducting the control.

For **FOS_POL.2**: Description of the management procedures to deal with malicious code with concrete actions and specifications and records on conducting the malicious code control.

For **FOS_POL.3**: Description of the management procedures to deal with mobile code with concrete actions and specifications and records on conducting the mobile code control.

For **FOS_POL.4**: Description of policy for use of cryptographic techniques and records on conducting the cryptographic control.

For **FOS_POL.5**: Description of protection procedures for publicly available systems with concrete actions and specifications and records on conducting the control.

B.3.1.4 FOS_POL.1 Security requirements

Dependencies: FOM_PRM.2 Segregation of privileges.

FOS_POL.1.1 The OSF shall define [assignment: *procedures*] on a software update management process to ensure the most up-to-date approved patches and application updates are installed for all authorized software.

FOS_POL.1.2 The OSF shall define [assignment: *procedures*] on identification of changes to information processing facilities and systems and assessment on potential impacts.

FOS_POL.1.3 The OSF shall define [assignment: *procedures*] for formal change control to control the implementation of changes to information processing facilities and systems.

FOS_POL.1.4 The OSF shall define [assignment: *procedures*] for maintenance and copying of program source libraries in accordance with change control.

FOS_POL.1.5 The OSF shall define [assignment: *procedures*] for the information systems to be regularly checked for compliance with security implementation standards.

FOS_POL.1.6 The OSF shall specify [assignment: *security controls*] in the statements of business requirements for new information systems, or enhancements to existing information systems.

FOS_POL.1.7 The OSF shall define [assignment: *procedures*] to control the installation of software on operational systems.

FOS_POL.1.8 The OSF shall define [assignment: *procedures*] that when operating systems are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security.

FOS_POL.1.9 The OSF shall define [assignment: *rules*] that modifications to software packages is discouraged, limited to necessary changes, and all changes are strictly controlled.

FOS_POL.1.10 The OSF shall document, maintain and make available [assignment: *procedures*] to all users who need them.

B.3.1.5 FOS_POL.2 Malicious code policy

Dependencies: no dependencies.

FOS_POL.2.1 The OSF shall define [assignment: *procedures*] for management to deal with malicious code protection on systems, reporting and recovering from malicious code attacks.

FOS_POL.2.2 The OSF shall define [assignment: *procedures*] for the detection of and protection against malicious code that may be transmitted through the use of communication facilities.

FOS_POL.2.3 The OSF shall define [assignment: *responsibilities*] to deal with malicious code protection on systems, training in their use, reporting and recovering from malicious code attacks.

FOS_POL.2.4 The OSF shall define [assignment: *procedures*] to implement detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness.

B.3.1.6 FOS_POL.3 Mobile code policy

Dependencies: no dependencies.

FOS_POL.3.1 The OSF shall define [assignment: *procedures*] for management to authorize the use of mobile code.

FOS_POL.3.2 The SSF shall define [assignment: *security requirements*] on the configuration of mobile code to ensure that authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code is prevented from executing.

B.3.1.7 FOS_POL.4 Cryptography policy

Dependencies: no dependencies.

FOS_POL.4.1 The OSF shall define [assignment: *a cryptographic policy*] on the use of cryptographic controls for protection of information in compliance with all relevant agreements, laws, and regulations.

FOS_POL.4.2 The OSF shall define [assignment: *a cryptographic policy*] on the use of cryptography controls for protection of information.

FOS_POL.4.3 The OSF shall define [assignment: *procedures*] for key management to support the organization's use of cryptographic techniques.

FOS_POL.4.4 The OSF shall define [assignment: *security requirements*] on legal advice before encrypted information or cryptographic controls are moved to another country.

FOS_POL.4.5 The SSF shall provide [assignment: *controls*] that any related cryptographic keys associated with encrypted archives or digital signatures are kept securely and made available to authorized persons when needed.

B.3.1.8 FOS_POL.5 Public systems

Dependencies: no dependencies.

FOS_POL.5.1 The SSF shall provide [assignment: *controls*] for the protection of software, data and other information requiring high level of integrity being made available on a publicly available system.

FOS_POL.5.2 The OSF shall provide [assignment: *security requirements*] for the publicly accessible system to be tested against weaknesses and failures prior to information being made available.

FOS_POL.5.3 The SSF shall provide [assignment: *security requirements*] that there is a formal approval process before information is made publicly available.

FOS_POL.5.4 The SSF shall provide [assignment: *security requirements*] that all input provided from the outside to the system is verified and approved.

B.3.2 Configuration of IT systems (FOS_CNF)

B.3.2.1 Family behaviour

This family defines configuration of IT system. It includes separation of development and operational environment, and system configuration.

B.3.2.2 Component levelling

FOS_CNF.1 Separation of development and operational environment. Separation of development and operational environment and access control are defined.

FOS_CNF.2 System configuration. Management of shared resources and system configuration are defined.

B.3.2.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOS_CNF.1**: Description on the separation of development and operational environment with concrete actions and specifications and records on conducting the control.

For **FOS_CNF.2**: Description of the management of shared resources and system configuration with concrete actions and specifications and records on conducting the control.

B.3.2.4 FOS_CNF.1 Separation of development and operational environment

Dependencies: no dependencies.

FOS_CNF.1.1 The OSF shall define [assignment: *rules*] on level of separation that is necessary, between operational, test and development environments, to prevent operational problems.

FOS_CNF.1.2 The OSF shall define [assignment: *rules*] for the transfer of software from development to operational status.

FOS_CNF.1.3 The SSF shall provide [assignment: *measures*] of access control that apply to operational application systems, to test application systems for protection of operational data.

FOS_CNF.1.4 The SSF shall provide [assignment: *controls*] of restrictions for IT support staff to access to program source libraries.

FOS_CNF.1.5 The OSF shall define [assignment: *rules*] development and operational software run on different systems or different processors.

FOS_CNF.1.6 The OSF shall define [assignment: *rules*] when operational information is copied to a test application system.

B.3.2.5 FOS_CNF.2 System configuration

Dependencies: no dependencies.

FOS_CNF.2.1 The OSF shall define [assignment: *rules*] segregation of groups of information services, users and information systems, on networks.

FOS_CNF.2.2 When a sensitive application is to run in a shared environment, the OSF shall define [assignment: *rules*] identification of the application systems with which it will share resources with the owner of the sensitive application.

FOS_CNF.2.3 The OSF shall define [assignment: *rules*] that sensitive systems have a dedicated (isolated) computing environment.

B.3.3 Network security of IT systems (FOS_NET)

B.3.3.1 Family behaviour

This family defines network security of IT systems. It includes specification of network security and network services.

B.3.3.2 Component levelling

FOS_NET.1 Network services. Network services and their access are defined.

FOS_NET.2 Network security. Protection of networks, security of information in networks, confidentiality and integrity of transmission data are defined.

B.3.3.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOS_NET.1**: Description on the network services with concrete actions and specifications and records on the access to the network.

For **FOS_NET.2**: Description of protection of networks, security of information in networks with concrete actions and specifications and records on the control.

B.3.3.4 FOS_NET.1 Network services

Dependencies: no dependencies.

FOS_NET.1.1 The OSF shall define [assignment: *rules*] for the networks and network services that are allowed to be accessed, authorization procedures for determining who is allowed to access which networks and networked services.

B.3.3.5 FOS_NET.2 Network security

Dependencies: no dependencies.

FOS_NET.2.1 The SSF shall provide [assignment: *controls*] to shut down inactive sessions in high risk locations after a defined period of inactivity.

FOS_NET.2.2 The SSF shall provide [assignment: *controls*] to clear the terminal screen and close both application and network sessions after a defined period of inactivity on a time-out facility.

FOS_NET.2.3 The SSF shall provide [assignment: *controls*] to make restrictions on connection times to provide additional security for high-risk applications.

FOS_NET.2.4 The SSF shall provide [assignment: *measures*] for linking network access rights to certain times of day or dates.

FOS_NET.2.5 The SSF shall provide [assignment: *controls*] to segregate groups of information services, users, and information systems on networks.

FOS_NET.2.6 The SSF shall provide [assignment: *controls*] to restrict the capability of users to connect to the network for shared networks, especially those extending across the organization's boundaries, in line with the access control policy and requirements of the business applications.

FOS_NET.2.7 The SSF shall provide [assignment: *controls*] to routing for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

B.3.4 Monitoring of IT systems (FOS_MON)

B.3.4.1 Family behaviour

This family defines monitoring of IT systems. It includes specification of audit log, legal advice, alarm and monitoring requirements.

B.3.4.2 Component levelling

FOS_MON.1 Audit logs. Audit requirements, audit management, production of audit, recorded information in the log and logging of system administrator are defined.

FOS_MON.2 Legal advice. Legal advice before implementing monitoring procedures is defined.

FOS_MON.3 Alarm requirements. Alarm parameter settings and alarm response are defined.

FOS_MON.4 Monitoring system use. Monitoring of system use is defined.

B.3.4.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOS_MON.1**: Description of the procedures for production of audit logs with concrete actions and specifications and records of audit logs in detail.

For **FOS_MON.2**: Description of the legal advice with concrete actions and specifications.

For **FOS_MON.3**: Description of alarm parameter settings and alarm response records with concrete actions and specifications and records on conducting the control.

For **FOS_MON.4**: Description of procedures for reviewing monitoring activities with concrete actions and specifications and records on conducting the reviews.

B.3.4.4 FOS_MON.1 Audit logs

Dependencies: no dependencies.

FOS_MON.1.1 The OSF shall plan [assignment: *security requirements*] for audit and activities involving checks on operational systems and agree to minimize the risk of disruptions to business processes.

FOS_MON.1.2 The OSF shall define [assignment: *security requirements*] on audit with appropriate management.

FOS_MON.1.3 The SSF shall produce [assignment: *logging*] of system administrator and system operator activities. Logs shall include time at which an event or failure occurred, information about the event or failure, which account and which administrator or operator was involved, all changes to equipment, software or procedures.

FOS_MON.1.4 The OSF shall define [assignment: *rules*] for recording of equipment logged out and logged back in when returned.

FOS_MON.1.5 The OSF shall define [assignment: *security requirements*] on logging of copying and use of operational information to provide an audit trail.

FOS_MON.1.6 The OSF shall define [assignment*: procedures*] on collection of audit trails and similar evidence.

FOS_MON.1.7 The OSF shall define [assignment: *security requirements*] on recording of a record of all removal of removable media from the organization to maintain an audit trail.

FOS_MON.1.8 The OSF shall establish [assignment: *procedures*] for monitoring use of information processing facilities and for reviewing the results of the monitoring activities regularly.

FOS_MON.1.9 The SSF shall provide [assignment: *security measures*] to protect logging facilities and log information against tampering and unauthorized access.

FOS_MON.1.10 The SSF shall produce [assignment: *procedures*] for logging of faults, analysis and appropriate action taken.

B.3.4.5 FOS_MON.2 Legal advice

Dependencies: no dependencies.

FOS_MON.2.1 The OSF shall define [assignment: *rules*] to take legal advice before implementing monitoring procedures.

B.3.4.6 FOS_MON.3 Alarm requirements

Dependencies: no dependencies.

FOS_MON.3.1 The SSF shall provide [assignment: *measures*] to alarm to the operational system.

FOS_MON.3.2 The SSF shall provide [assignment: *capabilities*] to set alarm parameters, pre-define alarm events and alarm changes of the alarm settings of the operational system.

FOS_MON.3.3 The OSF shall define [assignment: *rules and procedures*] that are defined for execution upon receipt of alarms and the required actions, including any timing constraints, responsible persons and reporting.

B.3.4.7 FOS_MON.4 Monitoring system use

Dependencies: no dependencies.

FOS_MON.4.1 The OSF shall provide [assignment: *procedures*] for monitoring use of information processing facilities and reviewing the results of the monitoring activities.

FOS_MON.4.2 The OSF shall define [assignment: *security requirements*] that the level of monitoring required for individual facilities is determined by a risk assessment.

B.3.5 Personnel control of IT systems (FOS_PSN)

B.3.5.1 Family behaviour

This family defines personnel controls for IT system. It includes specification of user authorization, malicious code, system use and facilities.

B.3.5.2 Component levelling

FOS_PSN.1 User authorization. User registration, user authentication and rules to keep authentication information such as passwords confidential are defined.

FOS_PSN.2 System use. Procedures to terminate active sessions are defined.

B.3.5.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOS_PSN.1**: Description of user registration, user authentication and rules to keep authentication information confidential with concrete actions and specifications and records on conducting the control.

For **FOS_PSN.2**: Description of procedures to terminate active sessions with concrete actions and specifications and records on conducting the control.

B.3.5.4 FOS_PSN.1 User authorization

Dependencies: FOM_PRM.2 Segregation of privilege

FOD_PSN.1 Personnel roles and responsibilities

FOD_PSN.3 Personnel agreement

FOS_PSN.1.1 The OSF shall define [assignment: *procedures*] for a formal user registration and de-registration for granting and revoking access to all information systems and services.

FOS_PSN.1.2 The OSF shall define [assignment: *procedures*] that include using unique user IDs so that users can be linked to and made responsible for their actions (the use of group IDs should only be permitted where they are suitable for the work carried out), checking that the user has authorization from the system owner to use the requested system or service in the access control procedure within the user registration and de-registration process.

FOS_PSN.1.3 The OSF shall define [assignment: *procedures*] that issue temporary authentication information following positive identification of the user when users forget or lose their authentication information. Temporary authentication information shall be passed to users in a secure manner.

FOS_PSN.1.4 The OSF shall define [assignment: *rules*] to prevent loss or compromise of authentication information, e.g. to avoid keeping a record of passwords unless this can be stored securely, select quality passwords with sufficient minimum length, not based on anything somebody else could easily guess or obtain using person related information, change passwords at regular intervals or based on the number of accesses and avoid re-using or cycling old passwords, change temporary passwords at the first log-on, do not include passwords in any automated log-on process and do not share individual user passwords.

FOS_PSN.1.5 The OSF shall define [assignment: *rules*] to sign a statement to prevent loss, compromise or misuse of authentication information e.g. to keep personal passwords confidential and work group passwords solely within the members of the group.

FOS_PSN.1.6 The SSF shall provide [assignment: *measures*] to provide users initially with secure temporary authentication information that they are forced to change or confirm immediately.

FOS_PSN.1.7 The OSF shall define [assignment: *rules*] that user authentication information is never stored on computer system in an unprotected form.

FOS_PSN.1.8 The OSF shall define [assignment: *a formal management process*] to control the allocation of authentication data to users.

B.3.5.5 FOS_PSN.2 System use

Dependencies: no dependencies.

FOS_PSN.2.1 The OSF shall define [assignment: *procedures*] to terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism.

FOS_PSN.2.2 The OSF shall define [assignment: *procedures*] to log-off mainframe computers, servers and office PCs when the session is finished.

FOS_PSN.2.3 The OSF shall define [assignment: *rules*] to use different user profiles for operational and test systems and menus.

FOS_PSN.2.4 The OSF shall define [assignment: *rules*] not to leave personal computers and computer terminals and printers logged on when unattended and protect them by key locks, passwords, or other controls when not in use.

B.3.6 Operational system assets of IT systems (FOS_OAS)

B.3.6.1 Family behaviour

This family defines the security of operational assets of IT systems. It includes specification of protection of operational assets, system program, back up and authentication information.

B.3.6.2 Component levelling

FOS_OAS.1 Protection of operational assets. Erasure of operational information, access control and secure keeping of system documentations are defined. Criteria for acceptance of new systems, rules of the use of utility program, authentication procedures for system utilities, procedures for updating of the operational software, rules not to use of unauthorized software and responsibility for following up vendors release of patches are defined.

FOS_OAS.2 Back-up procedures. Procedures to back-up copies of information and software are defined.

B.3.6.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOS_OAS.1**: Description of erasure of operational information, access control and secure keeping of system documentation with concrete actions and specifications and records on conducting the control. Description on criteria for acceptance of new systems, rules of the use of utility program, authentication procedures for system utilities, procedures for updating of the operational software, rules not to use of unauthorized software and responsibility for following up vendors release of patches with concrete actions and specifications and records on conducting the control.

For **FOS_OAS.2**: Description of procedures to back-up copies of information and software with concrete actions and specifications and records on conducting the control.

B.3.6.4 FOS_OAS.1 Protection of operational assets

Dependencies: FOS_POL.1 Security requirements

FOS_OAS.1.1 The OSF shall define [assignment: *rules*] for erase of operational information from a test application system immediately after the testing is complete.

FOS_OAS.1.2 The OSF shall define [assignment: *security requirements*] for control of program listings in a secure environment.

FOS_OAS.1.3 The SSF shall provide [assignment: *controls*] for protection and secure keeping of system documentation against unauthorized access.

FOS_OAS.1.4 The SSF shall provide [assignment: *controls*] not to make accessible compilers, editors and other development tools or system utilities from operational systems.

FOS_OAS.1.5 The OSF shall define [assignment: *acceptance criteria*] for new information systems and upgrades, and for new versions to be established and suitable tests carried out during development prior to acceptance.

FOS_OAS.1.6 The OSF shall define [assignment: *security requirements*] for detection, prevention and recovery to protect against malicious code and user awareness.

FOS_OAS.1.7 The OSF shall define [assignment: *rules*] to restrict and control use of utility programs that might be capable of overriding system and application controls.

FOS_OAS.1.8 The SSF shall provide [assignment: *controls*] for authentication for system utilities, segregation of system utilities from applications software, limitation of the use of system utilities to the minimum practical number of trusted, authorized users.

FOS_OAS.1.9 The OSF shall define [assignment: *procedures*] for the updating of the operational software, applications and program libraries by trained administrators upon appropriate management authorization.

FOS_OAS.1.10 The OSF shall define [assignment: *rules*] that only executable code is held on the operational system.

FOS_OAS.1.11 The OSF shall define [assignment: *rules*] that applications and operating system software are implemented after extensive and successful testing.

FOS_OAS.1.12 The OSF shall define [assignment: *rules*] that physical or logical access is only given to suppliers for support purposes when necessary, and with management approval.

FOS_OAS.1.13 The OSF shall define [assignment: *rules*] not to use of unauthorized software.

FOS_OAS.1.14 The OSF shall define [assignment: *responsibility*] for following up vendors releases of patches and fixes for application programs.

FOS_OAS.1.15 The OSF shall define [assignment: *procedures*] to upgrade to a new release taking into account the security of the release, the introduction of new security functionality or the number and severity of security problems affecting the current version.

FOS_OAS.1.16 The OSF shall define [assignment: *rules*] for the acceptable use of information and assets associated with information processing facilities to be identified, documented, and implemented.

B.3.6.5 FOS_OAS.2 Back-up procedures

Dependencies: no dependencies.

FOS_OAS.2.1 The SSF shall provide [assignment: *procedures*] to take and test back-up copies of information and software regularly in accordance with an agreed backup policy.

FOS_OAS.2.2 The OSF shall define [assignment: *procedures*] to produce necessary level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures.

FOS_OAS.2.3 The OSF shall define [assignment: *procedures*] for back-up media to ensure that they can be relied upon for emergency use when necessary.

FOS_OAS.2.4 The OSF shall define [assignment: *procedures*] to ensure they are effective and that they can be complete within time allotted in the operational procedures for recovery.

FOS_OAS.2.5 The OSF shall define [assignment: *security requirements*] on back-up arrangement for individual systems to ensure that they meet requirements of business continuity plans.

B.3.7 Records for IT systems (FOS_RCD)

B.3.7.1 Family behaviour

This family defines the records to be kept for IT systems. It includes specification of records.

B.3.7.2 Component levelling

FOS_RCD.1 Records. Recording of all suspected faults is defined.

B.3.7.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOS_RCD.1**: Description of all suspected faults with concrete actions and specifications and records on conducting the control.

B.3.7.4 FOS_RCD.1 Records

Dependencies: no dependencies.

FOS_RCD.1.1 The SSF shall provide [assignment: *measures*] for recording of all suspected or actual faults and corrective maintenance of equipment.

B.4 Class FOA: User Assets

This class provides operational control requirements for user assets of the operational system.

B.4.1 Privacy data protection (FOA_PRO)

B.4.1.1 Family behaviour

This family defines policy for user assets. It includes specification of privacy data, cryptography, management of user assets and roles and responsibilities.

B.4.1.2 Component levelling

FOA_PRO.1 Privacy data. Rules not to use operational databases containing personal information for testing, rules to obtain publicly available information in compliance with data protection legislation, and responsibilities of the owner of data to inform the authorised officer of the organization responsible for data protection are defined.

B.4.1.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOA_PRO.1**: Description of the rules not to use personal databases containing personal information, rules to obtain publicly available information in compliance with data protection legislation security policy, responsibility of the owner of the data to inform the authorised officer of the organization responsible for data protection with concrete actions and specifications and records on conducting the control.

B.4.1.4 FOA_PRO.1 Privacy data

Dependencies: no dependencies.

FOA_PRO.1.1 The OSF shall define [assignment: *rules*] not to use operational databases containing personal information for testing purposes.

FOA_PRO.1.2 The OSF shall define [assignment: *rules*] to obtain publicly available information in compliance with data protection legislation, to process completely and accurately in a timely manner and to protect during the collection process and when stored.

FOA_PRO.1.3 The OSF shall define [assignment: *responsibilities and rules*] of the owner of the data to inform the authorised officer of the organization responsible for data protection about any proposals to keep personal information, and to ensure awareness of the data protection principles defined in relevant legislation.

B.4.2 User assets information protection (FOA_INF)

B.4.2.1 Family behaviour

This family defines information protection for user assets. It includes data protection, procedures and rules.

B.4.2.2 Component levelling

FOA_INF.1 Data protection. Guidelines on the retention of records in transit, procedures to permit appropriate destruction of records and security for electronic communications are defined. Procedures for labelling and handling of information are defined.

B.4.2.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOA_INF.1**: Guidelines on the retention of records in transit, procedures to permit appropriate destruction of records and security for electronic communications with concrete actions and specifications. Description of procedures for labelling and handling of information with concrete actions and specifications and records on conducting the control.

B.4.2.4 FOA_INF.1 Data protection

Dependencies: FOS_POL.1 Security requirements

FOA_INF.1.1 The OSF shall define [assignment: *guidelines*] on the retention, storage, handling and disposal of records and information.

FOA_INF.1.2 The OSF shall define [assignment: *rules*] for a retention schedule identifying essential record types and the period of time for which they should be retained.

FOA_INF.1.3 The OSF shall define [assignment: *procedures*] to permit appropriate destruction of records after that period if they are not needed by the organization.

FOA_INF.1.4 The SSF shall provide [assignment: *measures*] that the information shall be destroyed, deleted or overwritten using approved techniques for devices containing sensitive information.

FOA_INF.1.5 The SSF shall provide [assignment: *measures*] for electronic communications by protecting messages from unauthorized access, modification or denial of services, ensuring correct addressing and transportation of the message, reliability and availability of the service, legal consideration.

FOA_INF.1.6 The OSF shall define [assignment: *procedures*] for labelling and handling for information including both in physical and electronic formats in accordance with classification scheme adopted by the organization.

FOA_INF.1.7 The OSF shall define [assignment: *rules*] for identification of privileges associated with each system product and each application, and the categories of staff to which they need to be allocated.

FOA_INF.1.8 The OSF shall define [assignment: *rules*] for allocation of privileges to users on a need-to-use basis and on an event-by-event basis in line with the access control policy.

FOA_INF.1.9 The OSF shall define [assignment: *security requirements*] to protect information involved in electronic commerce passing over public networks from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

B.5 Class FOB: Business

This class provides operational control requirements for business of the operational system.

B.5.1 Business policies (FOB_POL)

B.5.1.1 Family behaviour

This family defines business policies. It includes specification of security requirements and intellectual property.

B.5.1.2 Component levelling

FOB_POL.1 Security requirements. Business value of the information assets involved, security requirements of individual business applications, identification of all information related to the business applications and security roles and responsibilities for implementing and maintaining security polices are defined. Appropriate procedures to ensure compliance with legal restrictions on the use of material are defined.

B.5.1.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOB_POL.1**: Description of business value of the information assets involved, security requirements of individual business applications, identification of all information related to the business applications and security roles, responsibilities for implementing and maintaining security polices, appropriate procedures to ensure compliance with legal restrictions on the use of material with concrete actions and specifications and records on conducting the control.

B.5.1.4 FOB_POL.1 Security requirements

Dependencies: FOS_POL.1 Security requirements

FOB_POL.1.1 The OSF shall specify [assignment: *security policy*] to determine the business value of the system and information assets that form part of the overall system.

FOB_POL.1.2 The OSF shall define [assignment: *security requirements*] of individual business applications, identification of all information related to the business applications and the risks the information is facing, policies for information dissemination and authorization, consistency between the access control and information classification policies of different systems and networks, relevant legislation and any contractual obligations regarding protection of access to data or services, management of access rights in a distributed and networked environment which recognizes all types of connections available.

FOB_POL.1.3 The OSF shall define [assignment: *roles and responsibilities*] for implementing and maintaining security polices, for the protection of asset.

FOB_POL.1.4 The OSF shall define [assignment: *roles and responsibilities*] and communication to job candidates during the pre-assignment process.

FOB_POL.1.5 The OSF shall define [assignment: *procedures*] to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

FOB_POL.1.6 The OSF shall develop and implement [assignment: *policies and procedures*] to protect information associated with the interconnection of business information systems.

B.5.2 Business continuity (FOB_BCN)

B.5.2.1 Family behaviour

This family defines business continuity activities. It includes specification of business impact analysis, fault isolation and business continuity plans.

B.5.2.2 Component levelling

FOB_BCN.1 Impact analysis. Impact analysis for business continuity, business continuity plans to maintain or restore business operations, isolation of security faults and special access granted at the time of security faults are defined.

B.5.2.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOB_BCN.1**: Description of business continuity impact analysis, business continuity plans to maintain or restore business operations, fault isolation plans and special access granted at the time of security faults with concrete actions and specifications.

B.5.2.4 FOB_BCN.1 Impact analysis

Dependencies: FOD_RSM.1 Risk management within the organization

FOB_BCN.1.1 The OSF shall define [assignment: *security requirements*] on conducting a business impact analysis to identify events that can cause interruptions to business processes along with the probability and impact of such interruptions and their consequences for information security.

FOB_BCN.1.2 The OSF shall define [assignment: *security requirements*] on conducting business continuity impact analyses with full involvement from owners of business resources and processes.

FOB_BCN.1.3 The OSF shall define [assignment: *security requirements*] on business continuity plans for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements.

FOB_BCN.1.4 The OSF shall specify [assignment: *security requirements*] for understanding the risks the organization is facing in terms of their likelihood and their impact, understanding the impact which interruptions are likely to have on the business, formulating and documenting a business continuity strategy consistent with the agreed business objectives and priorities, formulating and documenting business continuity plans in line with the agreed strategy, regular testing and updating of the plans and processes put in place and ensuring that the management of business continuity is incorporated in the organization's processes and structure for business continuity.

FOB_BCN.1.5 The OSF shall define [assignment: *security requirements*] for development and implementation of business continuity plans to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

FOB_BCN.1.6 The OSF shall define [assignment: *procedures*] that a copy of the business continuity plans are stored in a remote location, at a sufficient distance to escape any damage from disaster at the main site. It shall be ensured that these copies are up-to-date and protected with the same security level as on the main site.

FOB_BCN.1.7 The OSF shall specify [assignment: *security requirements*] for the conditions for its activation, as well as the individuals responsible for executing each component of the plan for each business continuity plan.

FOB_BCN.1.8 The OSF shall define [assignment: *security requirements*] on testing and updating of business continuity plans to ensure that they are up to date and effective.

FOB_BCN.1.9 The OSF shall define [assignment: *security requirements*] on security faults isolation plans such that impact of a fault has minimal impact on business continuity on occurrence of security incidents.

FOB_BCN.1.10 The OSF shall define [assignment: *rules*] for special access to the operational system assets at the time of security faults.

FOB_BCN.1.11 The OSF shall define [assignment: *security requirements*] that a managed process is developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.

FOB_BCN.1.12 The OSF shall define [assignment: *security requirements*] for a single framework of business continuity plans to ensure that all plans are consistent, consistently address information security requirements, and identify priorities for testing and maintenance.

B.6 Class FOP: Facility and Equipment

This class provides operational control requirements for equipment, facilities and premises within the operational system.

B.6.1 Mobile equipment (FOP_MOB)

B.6.1.1 Family behaviour

This family defines mobile equipment security requirements. It includes specification of security requirements and roles and responsibilities.

B.6.1.2 Component levelling

FOP_MOB.1 Security requirements for mobile equipment. Requirements for physical protection and procedures to take care of security measures when using mobile computing facilities in public places are defined. Rules for the use of personal or privately owned information processing facilities and rules that unattended equipment are defined.

B.6.1.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOP_MOB.1**: Description of requirements for physical protection and procedures to take care of security measures when using mobile computing facilities in public places with concrete actions and specifications. Description of rules for the use of personal or privately owned information processing facilities and rules that unattended equipment with concrete actions and specifications and records on conducting the control.

B.6.1.4 FOP_MOB.1 Security requirements for mobile equipment

Dependencies: no dependencies.

FOP_MOB.1.1 The OSF shall define [assignment: *security requirements*] for risks of working with mobile computing equipment in unprotected environments in the mobile computing policy.

FOP_MOB.1.2 The OSF shall define [assignment: *security requirements*] for physical protection, access controls, cryptographic techniques, back-ups, and virus protection in the mobile computing policy.

FOP_MOB.1.3 The SSF shall provide [assignment: *measures*] to protect against risks of using mobile computing facilities.

FOP_MOB.1.4 The OSF shall define [assignment: *procedures*] to take care of security measures when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. The OSF shall give suitable protection to the use of mobile facilities connected to networks.

FOP_MOB.1.5 The SSF shall provide [assignment: *measures*] for the protection of mobile computing facilities by physical protection from theft especially when left unattended.

FOP_MOB.1.6 The OSF shall define [assignment: *rules*] for the use of personal or privately owned information processing facilities for processing business information.

FOP_MOB.1.7 The OSF shall define [assignment: *rules*] that unattended equipment and media at the premises should not be left in public places and that portable computers shall be carried as hand luggage and disguised where possible when travelling.

B.6.2 Removable equipment (FOP_RMM)

B.6.2.1 Family behaviour

This family defines security procedures for removable equipment. It includes specification of management of removable media.

B.6.2.2 Component levelling

FOP_RMM.1 Management of Removable Media. Procedures for the management of removable computer media, procedures on authorization for media removed from the organization and procedures for erase of the contents of any re-usable media are defined.

B.6.2.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOP_RMM.1**: Description of procedures for the management of removable computer media, procedures on authorization for media removed from the organization and procedures for erase of the contents of any re-usable media, with concrete actions and specifications and records on conducting the control.

B.6.2.4 FOP_RMM.1 Management of Removable Media

Dependencies: no dependencies.

FOP_RMM.1.1 The OSF shall define [assignment: *procedures*] for the management of removable computer media.

FOP_RMM.1.2 The OSF shall define [assignment: *procedures*] on authorization for media removed from the organization.

FOP_RMM.1.3 The OSF shall define [assignment: *procedures*] for minimization of risks concerning with leakage of sensitive information to unauthorized persons for establishment of formal procedures for the secure disposal of media.

FOP_RMM.1.4 The OSF shall define [assignment: *procedures*] for erasure of the contents, including any sensitive data and licensed software, of any re-usable media and equipment containing storage media that are to be removed from the organization when no longer required and to check them for completion.

B.6.3 Remote equipment (FOP_RMT)

B.6.3.1 Family behaviour

This family defines security procedures for remote equipment. It includes specification of management of remote equipment.

B.6.3.2 Component levelling

FOP_RMT.1 Management of Remote Equipment. Responsibilities and procedures for the management and use of remote equipment and the procedures for remote access to business information are defined.

B.6.3.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOP_RMT.1**: Description of responsibilities and procedures for the management and use of remote equipment and the procedures for remote access to business information with concrete actions and specifications and records on conducting the control.

B.6.3.4 FOP_RMT.1 Management of Remote Equipment

Dependencies: no dependencies.

FOP_RMT.1.1 The OSF shall define [assignment: *responsibilities and procedures*] for the management and use of remote equipment including equipment in user areas.

FOP_RMT.1.2 The OSF shall define [assignment: *procedures*] for remote access to business information across public network using mobile computing facilities only after successful identification and authentication, and with suitable access control mechanisms.

FOP_RMT.1.3 The SSF shall provide [assignment: *measures*] for a key lock or an equivalent control for secure PCs or terminals from unauthorized use.

FOP_RMT.1.4 The SSF shall provide [assignment: *measures*] for automatic equipment identification as a means to authenticate connections from specific locations and equipment.

FOP_RMT.1.5 The SSF shall provide [assignment: *controls*] for physical and logical access to diagnostic and configuration ports.

B.6.4 System equipment (FOP_SYS)

B.6.4.1 Family behaviour

This family defines security procedures for system equipment. It includes specification of management of system equipment.

B.6.4.2 Component levelling

FOP_SYS.1 Management of System Equipment. Site fallback equipment and back-up media, rules to keep hazardous or combustible materials, procedures to inspect incoming material and protection of network cabling are defined.

B.6.4.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOP_SYS.1**: Description of site fallback equipment and back-up media, rules to keep hazardous or combustible materials, procedures to inspect incoming material and protection of network cabling with concrete actions and specifications.

B.6.4.4 FOP_SYS.1 Management of System Equipment

Dependencies: no dependencies.

FOP_SYS.1.1 The OSF shall define [assignment: *rules*] for site fallback equipment and back-up media at a safe distance to avoid damage from a disaster at the main site.

FOP_SYS.1.2 The OSF shall define [assignment: *rules*] to keep hazardous or combustible materials securely at a safe distance from a secure area.

FOP_SYS.1.3 The OSF shall define [assignment: *rules*] to keep directories and internal telephone books identifying locations of sensitive information processing facilities not accessible by the public.

FOP_SYS.1.4 The OSF shall define [assignment: *procedures*] to inspect incoming material for potential threats before it is moved from the delivery and loading area to the point of use.

FOP_SYS.1.5 The SSF shall provide [assignment: *measures*] for protection of network cabling from unauthorized interception or damage through public areas.

FOP_SYS.1.6 The OSF shall define [assignment: *rules*] to maintain equipment in accordance with supplier's recommended service intervals and specifications.

FOP_SYS.1.7 The OSF shall define [assignment: *rules*] that only authorized maintenance personnel should carry out repairs and service equipment.

FOP_SYS.1.8 The OSF shall define [assignment: *controls*] for an appropriate level of physical and environmental protection consistent with the standards applied at the main site for back-up information. Controls applied to media at the main site shall be extended to cover the back-up site.

FOP_SYS.1.9 The OSF shall define [assignment: *rules*] for keeping of all media in a safe and secure environment in accordance with manufactures' specification.

FOP_SYS.1.10 The OSF shall define [assignment: *responsibilities*] for protecting unattended equipment for all employees, contractors and third party users of the security requirements and procedures.

FOP_SYS.1.11 The OSF shall define [assignment: *procedures*] to ensure that all relevant information is transferred to the organization and securely erased from the equipment, in case where an employee or contractor or third party user purchase the organization's equipment or uses their own personal equipment.

FOP_SYS.1.12 The OSF shall provide [assignment: *controls*] for media containing information to be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.

B.6.5 Facility Management (FOP_MNG)

B.6.5.1 Family behaviour

This family defines management of facilities. It includes specifications of physical security, supporting utilities, and communications links.

B.6.5.2 Component levelling

FOP_MNG.1 Physical security. Physical security for offices, rooms and facilities is defined. Separation of development, test and operational facilities is defined. Requirements for adequate back-up facilities, and protection of information processing facilities are defined.

FOP_MNG.2 Power supporting utilities. The control of supporting utilities and the use of a back-up generator are defined.

FOP_MNG.3 Communications links. The control of external communications links is defined.

B.6.5.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOP_MNG.1**: Description of physical security for offices, rooms and facilities, separation of development, test and operational facilities, adequate back-up facilities, and protection of information processing facilities, with concrete actions and specifications.

For **FOP_MNG.2**: Description of the control of power supporting utilities and the use of back-up generators with concrete actions and specifications.

For **FOP_MNG.3**: Description of the control of communications links and failure arrangements with concrete actions and specifications.

B.6.5.4 FOP_MNG.1 Physical security

Dependencies: FOD_PSN.5 Access to facility and equipment

FOP_MNG.1.1 The OSF shall define [assignment: *security requirements*] on physical security for offices, rooms and facilities] against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.

FOP_MNG.1.2 The OSF shall define [assignment: *security requirements*] for separation of development, test and operational facilities to reduce risks of unauthorized access or changes to the operational system.

FOP_MNG.1.3 The OSF shall define [assignment: *security requirements*] for adequate back-up facilities to ensure that all essential information and software can be recovered following a disaster or media failure.

FOP_MNG.1.4 The OSF shall define [assignment: *security requirements*] for protection of information processing facilities to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities.

B.6.5.5 FOP_MNG.2 Power supporting utilities

Dependencies: no dependencies.

FOP_MNG.2.1 The SSF shall provide [assignment: *controls*] for protection of equipment from power failures and other disruptions caused by failures in supporting utilities.

FOP_MNG.2.2 The OSF shall define [assignment: *security requirements*] for the use of UPS (Uninterruptible Power Supply) equipment.

FOP_MNG.2.3 The OSF shall define [assignment: *security requirements*] for the use of a back-up generator if processing is to continue in case of a prolonged power failure.

B.6.5.6 FOP_MNG.3 Communications links

Dependencies: no dependencies.

FOP_MNG.3.1 The SSF shall provide [assignment: *controls*] for protection of power and telecommunications cabling carrying data or supporting information services from interception or damage.

FOP_MNG.3.2 The SSF shall define [assignment: *security requirements*] for ensuring that communications connectivity can be maintained in the event of communications equipment failure or interruption.

B.7 Class FOT: Third parties

This class provides operational control requirements for third parties.

B.7.1 Third party management (FOT_MNG)

B.7.1.1 Family behaviour

This family defines management of third parties and commitments for third parties. It includes specification of outsourcing and third party security requirements.

B.7.1.2 Component levelling

FOT_MNG.1 Outsourcing. A plan for the necessary transitions of information, licensing arrangements, code ownership and intellectual property rights are defined.

FOT_MNG.2 Third party security requirements. All security requirements resulting from work with third parties are defined. Sufficient overall control and rules not to provide access to the organization's information are defined. Risk management applicable to third party relationships is defined.

B.7.1.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOT_MNG.1**: Description of a plan for the necessary transitions of information, licensing arrangements, code ownership and intellectual property rights with concrete actions and specifications.

For **FOT_MNG.2**: Description of all security requirements resulting from work with third parties, sufficient overall control and rules not to provide access to the organization's information and risk management with concrete actions and specifications.

B.7.1.4 FOT_MNG.1 Outsourcing

Dependencies: FOD_PSN.3 Personal agreement.

FOT_MNG.1.1 The OSF shall define [assignment: *security requirements*] on a plan for the necessary transitions of information, information processing facilities and anything else that needs to be moved and security maintenance in the transition period for arrangement of outsourcing.

FOT_MNG.1.2 The OSF shall define [assignment: *security requirements*] for licensing arrangements, code ownership and intellectual property rights, certification of the quality and accuracy of the work carried out, escrow arrangements in the event of failure of the third party, rights of access for audit of the quality and accuracy of work done, contractual requirements for quality of code and testing before installation to detect Trojan code where software development is outsourced.

B.7.1.5 FOT_MNG.2 Third party security requirements

Dependencies: no dependencies.

FOT_MNG.2.1 The OSF shall define [assignment: *security requirements*] resulting from work with third parties or internal controls in the agreement with the third party.

FOT_MNG.2.2 The OSF shall define [assignment: *security requirements*] to ensure compliance with organization's security policies and standards in the agreement with third parties involving accessing, processing, communicating or managing organizational information or information processing facilities.

FOT_MNG.2.3 The OSF shall define [assignment: *security requirements*] for sufficient overall control and security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a third party.

FOT_MNG.2.4 The OSF shall define [assignment: *rules*] not to provide access to the organization's information by third parties until the controls are in place and an agreement has been signed defining the terms and conditions for the connection or access and the working arrangement.

FOT_MNG.2.5 The OSF shall define [assignment: *security requirements*] for conduct of risk management of business processes with third parties and third party personnel.

FOT_MNG.2.6 The OSF shall define [assignment: *security requirements*] for conduct of risk management of the different means of storing and processing information that the third party will employ.

FOT_MNG.2.7 The OSF shall define [assignment: *procedures*] for outsourced software development to be supervised and monitored by the organization.

FOT_MNG.2.8 The OSF shall define [assignment: *security requirements*] to confirm that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

FOT_MNG.2.9 The OSF shall define [assignment: *security requirements*] that the services, reports and records provided by the third party are regularly monitored and reviewed, and audits carried out regularly.

FOT_MNG.2.10 The OSF shall define [assignment: *security requirements*] that changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, is managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

FOT_MNG.2.11 The OSF shall define [assignment: *security requirements*] to be covered in the agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities.

B.8 Class FOM: Management

This class provides requirements for management of operational controls.

B.8.1 Management of security parameters (FOM_PRM)

B.8.1.1 Family behaviour

This family defines management of security parameters. It includes specification of use of cryptography and privileges.

B.8.1.2 Component levelling

FOM_PRM.1 Use of cryptography. The approach to key management including methods to deal with the protection of cryptographic keys and recovery of encrypted information are defined.

FOM_PRM.2 Segregation of privileges. Segregation of privileges is defined.

B.8.1.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOM_PRM.1**: Description of the approach to key management including methods to deal with the protection of cryptographic keys and recovery of encrypted information with concrete actions and specifications.

For **FOM_PRM.2**: Description of segregation of privileges with concrete actions and specifications.

B.8.1.4 FOM_PRM.1 Use of cryptography

Dependencies: FOS_POL.4 Cryptography policy.

FOM_PRM.1.1 The OSF shall define [assignment: *security requirements*] on management approach towards the use of cryptographic controls across the organization, the approach to key management including methods to deal with the protection of cryptographic keys and recovery of encrypted information in the case of lost, compromised or damaged keys, roles and responsibilities, who is responsible for the implementation of the policy; and regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information for the organization's cryptographic policy.

B.8.1.5 FOM_PRM.2 Segregation of privileges

Dependencies: no dependencies.

FOM_PRM.2.1 The OSF shall define [assignment: *rules*] for segregation of privileges to reduce opportunities for unauthorized modification or misuse of assets, separation of the initiation of an event from its authorization.

FOM_PRM.2.2 The OSF shall define [assignment: *security requirements*] on assignment of privileges to a different user identity from those used for normal business use.

B.8.2 Management of asset classification (FOM_CLS)

B.8.2.1 Family behaviour

This family defines classification of assets. It includes categorization.

B.8.2.2 Component levelling

FOM_CLS.1 Categorization. Categorization of records is defined.

FOM_CLS.2 Asset Identification. Asset identification is defined.

B.8.2.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOM_CLS.1**: Description of categorization of records with concrete specifications.

For **FOM_CLS.2**: Description of asset identification with concrete specifications.

B.8.2.4 FOM_CLS.1 Categorization

Dependencies: no dependencies.

FOM_CLS.1.1 The OSF shall define [assignment: *security requirements*] on categorization of records into record types, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of storage media.

B.8.2.5 FOM_CLS.2 Asset Identification

Dependencies: no dependencies.

FOM_CLS.2.1 The OSF shall define [assignment: *security requirements*] on specification of identification, specification the type of asset, the asset function, requirements for management, provide levels of protection commensurate with the importance of the assets agree ownership and security classification and record current location in an inventory to each asset.

FOM_CLS.2.2 The OSF shall define [assignment: *security requirements*] on drawing up and maintenance of an inventory of all important assets.

FOM_CLS.2.3 The OSF shall define [assignment: *security requirements*] on retention period for essential business information, and also any requirements for archive copies to be permanently retained.

B.8.3 Management of personnel security responsibilities (FOM_PSN)

B.8.3.1 Family behaviour

This family defines the security responsibilities of staff. It includes asset owners and security managers.

B.8.3.2 Component levelling

FOM_PSN.1 Asset ownership. Asset ownership is defined.

FOM_PSN.2 Security managers. Assignment of security managers is defined.

B.8.3.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOM_PSN.1**: Description of asset ownership with concrete specifications.

For **FOM_CLS.2**: Description of assignment of security managers with concrete specifications.

B.8.3.4 FOM_PSN.1 Asset ownership

Dependencies: FOA_POL.3 Management of user assets

FOM_PSN.1.1 The OSF shall define [assignment: *security requirements*] that all information and assets associated with information processing facilities is owned by a designated part of the organization.

B.8.3.5 FOM_PSN.2 Security managers

Dependencies: no dependencies.

FOM_PSN.2.1 The OSF shall define [assignment: *security requirements*] on assignment of a specific responsible manager for each security control].

FOM_PSN.2.2 The OSF shall define [assignment: *security requirements*] that management requires employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

B.8.4 Management of security organization (FOM_ORG)

B.8.4.1 Family behaviour

This family defines organization of security management. It includes security management responsibilities and management forum membership.

B.8.4.2 Component levelling

FOM_ORG.1 Management responsibilities. Management responsibilities for security are defined.

FOM_ORG.2 Management forum membership. Membership of the management forum is defined.

B.8.4.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOM_ORG.1**: Description of management responsibilities with concrete actions and specifications.

For **FOM_ORG.2**: Description of management forum membership with concrete specifications.

B.8.4.4 FOM_ORG.1 Management responsibilities

Dependencies: FOD_ORG.1 Security coordination responsibilities

FOM_ORG.1.1 The OSF shall define [assignment: *responsibilities*] for management to ensure security activities comply with the security policy, approve specific methodologies and processes for information security, monitor significant threat changes and exposure of information assets to threat, assess the adequacy and coordinate the implementation of specific information security controls for new systems or services, promote the visibility of support for information security throughout the organization.

FOM_ORG.1.2 The OSF shall define [assignment: *responsibilities*] for managers to ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

FOM_ORG.1.3 The OSF shall define [assignment: *responsibilities*] for the management to review the information security policy at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

B.8.4.5 FOM_ORG.2 Management forum membership

Dependencies: FOD_ORG.2 Management forum responsibilities

FOM_ORG.2.1 The OSF shall define [assignment: *appointment of representatives from management and from different parts of the organization group with relevant roles and job functions*] to the management forum to ensure that information security activities are coordinated.

B.8.5 Management of security reporting (FOM_INC)

B.8.5.1 Family behaviour

This family defines management of reporting of security incidents. It includes management of reported security problems.

B.8.5.2 Component levelling

FOM_INC.1 Reporting detected security problems. Management of reported security problems is defined.

B.8.5.3 Records

The operational system shall maintain and make available for inspection the following evidence.

For **FOM_INC.1**: Description of security reporting procedures with concrete actions and specifications and records on conducting the control.

B.8.5.4 FOM_INC.1 Reporting detected security problems

Dependencies: no dependencies.

FOM_INC.1.1 The OSF shall define [assignment: *procedures*] to note and report any observed or suspected security weaknesses in, or threats to, systems or services to their management or directly to their service provider as quickly as possible in order to prevent security incidents.

FOM_INC.1.2 The OSF shall define [assignment: *rules*] to prohibit attempting to prove a suspected weakness exists through attempted exploitation.

Annex C
(normative)

Operational system assurance requirements

C.1 Introduction

This annex defines the additional assurance requirements for operational systems needed in addition to those defined in ISO/IEC 15408-3. ISO/IEC 15408-3 is used as the basis for the structure for these components.

Security assurance can be considered from two aspects, correctness and effectiveness. Correctness means that the security mechanisms have been implemented correctly; that they work in accordance with the security specifications, and that availability of security services is maintained. Effectiveness means that security mechanisms work against security threats and vulnerabilities and prevent unauthorized processes, such as bypass of security mechanisms or unauthorized interference with security mechanisms. Assurance can be gained from activities across all phases of the system life cycle. This concept is illustrated in Table C.1 following.

Both correctness and effectiveness can be assessed by security evaluation. In addition, other forms of assurance may need to be taken into account, such as assurance associated with the system developer's reputation, and assurance derived from the maturity of the system development processes used. More information on this topic can be found in ISO/IEC TR 15443 [3].

Many aspects of operational systems assurance are covered by existing ISO/IEC 15408-3 evaluation criteria. However, there are some aspects of operational systems assurance for which additional criteria are required.

Nine new classes of assurance requirements are defined in this annex. They are:

a) SPP evaluation (ASP), which validates System Protection Profiles;

b) SST evaluation (ASS), which validates System Security Targets;

c) Operational system guidance document (AOD), which validates Operational system guidance document;

d) Operational system architecture design and configuration documentation (ASD), which validates Operational system architecture design and configuration documentation;

e) Operational system configuration management (AOC), which validates Operational system configuration management;

f) Operational system test (AOT), which validates Operational system test;

g) Operational system vulnerability analysis (AOV), which validates Operational system vulnerability analysis;

h) Operational system life cycle support (AOL), which validates Operational system life cycle support;

i) System security installation (ASI), which validates System security installation;

j) Records on operational system (ASO), which validates records and monitoring of operational controls.

Table C.1 — Assurance for operational systems

Factors	Life cycle Stage	Assurance Objectives	Assurance Class/Family	Evaluation Activities
Effectiveness	Development/ Integration	Risk Counteraction *Security requirements specified in the SST are effective in reducing unacceptable risks to a tolerable level.*	SST/SPP evaluation (AST/ASP)	Security objectives shall address all risks identified as unacceptable Security requirements shall correspond to security objectives Security countermeasures shall meet the STOE Summary Specification
		Operational system architecture *Security countermeasures of subsystems, components etc. work together to create required secure properties for the overall system.*	Operational system architecture description (ASD_SAD) Subsystem design (ASD_SSD) Component design (ASD_CMP) Implementation representations (ASD_IMP) Security interfaces (ASD_IFS) Security concept of operations (ASD_CON)	Security countermeasures shall work effectively in combination with other countermeasures.
		Secure development environment	Security measures and their verification on development environment (AOL_DVS)	Security measures for development environment shall be confirmed.
	Installation	Strength of Security Mechanisms *Strength of security mechanisms are effective for the system.*	Vulnerability analysis (AOV_VLA)	Vulnerability analysis shall be conducted and the vulnerabilities shall not be exploitable by the assumed attack potential. Penetration testing shall be conducted and there shall be no security problems.
		Communication and awareness training *Rules and procedures are communicated and trained to appropriate personnel effectively.*	Confirmation of communication and awareness (ASI_CMM, ASI_AWA)	Communication and awareness shall be confirmed by records and interview.
	Operation	Monitoring of Security Countermeasures *Audit logs and monitoring records are collected to show security countermeasures operate as intended.*	Detection of insecure state (AOV_MSU) Verification of operation of SSF (AOD_ADM, AOD_USR, AOD_OCD, ASI_AWA, ASI_CMM, ASO_RCD, ASO_VER)	Security countermeasures shall be confirmed as operating as intended.
		Verification *It is confirmed that no risks are detected that should be countered and security controls perform as expected.*		It shall be confirmed by audit logs and interviews that no unacceptable risks are detected.

Factors	Life cycle Stage	Assurance Objectives	Assurance Class/Family	Evaluation Activities
	Modification	Regression testing *Security controls continue to work as intended.*	Regression testing (AOT_REG)	Detected security problems shall be investigated and results fed back.
		Penetration testing *System changes do not introduce gaps in the coverage of security controls.*	Penetration testing (AOV_VLA) Testing for insecure states (AOV_MSU)	Detected security problems shall be investigated and results fed back.
Correctness	Development/ Integration	Correspondence between Security Risks and Security Requirements, and between Security Requirements and Security Countermeasures. *Security requirements address all unacceptable risks. Security countermeasures meet all security requirements*	SST/SPP evaluation (AST/ASP)	Security objectives shall address all risks identified as unacceptable Security requirements shall correspond to security objectives Security countermeasures shall meet the STOE Summary Specification
		Configuration Management *Security countermeasure configuration items are managed correctly.*	Configuration (AOD_OCD)	Configuration items shall be managed and applied to the system.
		Correspondence with Development Works *Security countermeasures are implemented correctly.* *Security countermeasures →distribution→ implementation*	Operational system architecture description (ASD_SAD) Subsystem design (ASD_SSD) Component design (ASD_CMP) Implementation representations (ASD_IMP) Security interfaces (ASD_IFS) Security concept of operations (ASD_CON) Testing (AOT)	Security countermeasures shall be implemented without unauthorized modification, addition or deletion.
		Guidance Documents Description *Secure operations are described in the guidance documents correctly.*	Description (AOD_ADM, AOD_USR)	Operation of security countermeasures shall be sufficiently described.

Factors	Life cycle Stage	Assurance Objectives	Assurance Class/Family	Evaluation Activities
	Installation	Compliance *Operational controls are compliant with security requirements.*	Examination of guidance (AOV_MSU)	Guidance shall be clear and complete.
		Authorization *Installation of operational controls is authorized by an authorized person.*	(none)	(none)
		Configuration *Components and subsystems are configured correctly*	Configuration (AOC) Testing (AOT)	Component and subsystem configuration and operation of controls shall be verified
		Start up *STOE Start up executes correctly*	Installation and start up (ASI_SIC)	Correct installation and start up shall be confirmed
	Operation	Monitoring of Security Countermeasures Security countermeasures are operated correctly.	Monitoring (ASO_MON)	Audit trails and monitoring records on access to and utilization of assets shall be inspected.
		Verification *It is confirmed that no risks are detected that should be countered and security controls perform as expected.*	Verification of configuration (AOC_OBM) Verification of operational environment (AOC_ECP, AOC_PPC, AOC_NCP) Verification of secure installation (AOC_SIC) Verification of records (ASO_RCD) Independent verification (ASO_VER)	Security controls shall be verified
	Modification	Design verification *It is confirmed that modifications have not invalidated other parts of the design*	Design verification (AOD_GVR, ASD_GVR)	Design changes shall be analysed.
		Regression testing *It is confirmed that changed security controls work as intended*	Regression testing (AOT_REG)	Detected security problems shall be investigated and results fed back.

There are new assurance classes for the evaluation of System Protection Profiles (SPP) and System Security Targets (SST), since the contents of an SPP or SST are expanded from those of a product PP or ST. The other new classes address the additional assurance requirements for operational systems evaluation. The relationship between the additional assurance requirements defined in this annex and the four life cycle stages is shown in Table C.2 following.

Table C.2 — Assurance requirements and the operational system life cycle

Life cycle	Assurance requirement	
Development/ Integration	AOD_OCD.1	Description of the configuration in the Configuration guidance
	AOD_ADM.1	Description of administrator related SSFs in the Administrator guidance
	AOD_USR.1	Description of user related SSFs in the User guidance
	ASD_SAD.1	Description of the architecture
	ASD_IFS.1	Description of the external interfaces
	ASD_SSD.1	Description of the structure of subsystems
	ASD_CMP.1	Description of the structure of primitive component
	ASD_IMP.1	Production of the specific implementation representation
	ASD_CON.1	Security concept of operations
	AOL_DVS.1	Security measures for development environment
	AOT_FUN.1	Functional test for SSFs
	AOT_COV.1	Test coverage for SSFs
	AOT_COV.2	Completeness of test coverage for SSFs
	AOT_DPT.1	Test depth for interface specification
	AOT_DPT.2	Test depth for subsystem design
	AOT_DPT.3	Test depth for component design
	AOT_DPT.4	Test depth for implementation representation
	AOL_DVS.2	Verification of Security measures for development environment
Installation	AOC_OBM.1	Configuration management
	AOC_ECP.1	Identification of evaluated products
	AOC_PPC.1	Identification of conformance with PPs
	AOC_NCP.1	New evaluation for new products
	AOT_FUN.1	Functional test for SSFs
	AOT_COV.1	Test coverage for SSFs
	AOT_COV.2	Completeness of test coverage for SSFs
	AOT_DPT.1	Test depth for interface specification
	AOT_DPT.2	Test depth for subsystem design
	AOT_DPT.3	Test depth for component design
	AOT_DPT.4	Test depth for implementation representation
	AOT_IND.1-3	Independent testing
	AOV_MSU.1	Examination of operational system guidance
	AOV_VLA.1-4	Penetration testing
	ASI_AWA.1	Awareness training
	ASI_CMM.1	Communication on SSFs to appropriate personnel
	ASI_SIC.1	Secure installation and start up of STOE

Life cycle	Assurance requirement	
Operation	AOD_OCD.2	Verification of specifications in the Configuration guidance
	AOD_ADM.2	Verification of conduction on SSFs in the Administrator guidance
	AOD_USR.2	Verification of conduction on SSFs in the User guidance
	AOC_OBM.2	Verification of configuration management
	AOC_ECP.2	Verification of operational environment for the evaluated products
	AOC_PPC.2	Verification of operational environment for claimed conformance with PPs
	AOC_NCP.2	Verification of operational environment for the new evaluated products
	AOV_MSU.2	Detection of insecure operational states and recoveries
	ASI_AWA.2	Verification of awareness training
	ASI_CMM.2	Verification of communication on SSFs to personnel
	ASI_SIC.2	Verification of secure installation and start up
	ASO_RCD.1-2	Verification of operational records
	ASO_VER.1-2	Verification of operational controls
	ASO_MON.1	Management monitoring for SSFs
	ASO_MON.2	Independent verification of management monitoring
Modification	AOD_GVR.1	Guidance document verification
	ASD_GVR.1	Design verification
	AOT_REG.1	Regression testing
	AOV_MSU.2	Analysis and testing for insecure states
	AOV_VLA.1-4	Penetration testing

There are two presentational differences in this annex from ISO/IEC 15408-3. Developer action elements have been renamed as developer/integrator action elements, in order to recognise that an operational system may be composed by a system integrator who is distinct from the developer of components and products used within the system, and both of these may collaborate in the production and delivery of the necessary evidence. In some cases it is operational system management who are responsible for the production of evidence and so in these families the action elements to provide evidence are identified as management actions.

The dependencies between assurance components are shown in Tables C.3 to C.5 below. Three tables have been used, as SPP, SST and STOE evaluation are performed independently, and therefore there can be no interdependencies between each set. Each of the components that is a dependency of some assurance component is allocated a column. Each assurance component with dependencies is allocated a row. The value in the table cell indicates whether the column label component is directly required (indicated by a cross “X”), or indirectly required (indicated by a dash “-”) by the row label component.

Table C.3 — SPP assurance dependencies

	ASP_INT.1	ASP_ECD.1	ASP_SPD.1	ASP_OBJ.1	ASP_REQ.1	ASP_DMP.1	ASP_DMO.1	ASP_DMR.1
ASP_CCL.1	X	X	X	X	X			
ASP_OBJ.1			X					
ASP_REQ.1		X						
ASP_REQ.2		X	-	X				
ASP_DMI.1	X							
ASP_DMC.1	-	-				X	X	X
ASP_DMO.1	X					X		
ASP_DMR.1		X						
ASP_DMR.2	-	X				-	X	

Table C.4 — SST assurance dependencies

	ASS_INT.1	ASS_ECD.1	ASS_SPD.1	ASS_OBJ.1	ASS_REQ.1	ASS_DMI.1	ASS_DMP.1	ASS_DMO.1	ASS_DMR.1
ASS_CCL.1	X	X	X	X	X				
ASS_OBJ.1			X						
ASS_REQ.1		X							
ASS_REQ.2		X	-	X					
ASS_TSS.1	X	-			X				
ASS_DMI.1	X								
ASS_DMC.1	-	-					X	X	X
ASS_DMO.1	X						X		
ASS_DMR.1		X							
ASS_DMR.2	-	X					-	X	
ASS_DMS.1	-	-				X			X

Table C.5 — STOE assurance dependencies

	AOD_OCD.1	AOD_ADM.1	AOD_USR.1	ASD_SAD.1	ASD_IFS.1	ASD_SSD.1	ASD_CMP.1	ASD_IMP.1	ASD_CON.1	AOC_OBM.1	AOT_FUN.1
AOD_OCD.1/2				-	-	-	X		X		
AOD_ADM.1/2				X							
AOD_USR.1/2				X							
AOD_GVR.1	X	X	X	-	-	-	-		-		
ASD_IFS.1				X							
ASD_SSD.1				X	X						
ASD_CMP.1				-	X	X					
ASD_IMP.1				-	-	-	X				
ASD_CON.1				X							
ASD_GVR.1				X	X	X	X		X		
AOC_ECP.1/2										X	
AOC_PPC.1/2										X	
AOC_NCP.1/2										X	
AOT_COV.1/2				-	X						X
AOT_DPT.1				-	X						X
AOT_DPT.2				-	X	X					X
AOT_DPT.3				-	X	X	X				X
AOT_DPT.4				-	X	X	X	X			X
AOT_IND.1		X	X	-	X						
AOT_IND.2/3		X	X	-	X						X
AOV_MSU.1/2		X	X	-							
AOV_VLA.1		X	X	-	X	X			X		
AOV_VLA.2/3/4		X	X	-	X	X	-	X	X		

C.2 Class ASP: System Protection Profile evaluation

C.2.1 Introduction

This clause provides assurance criteria for the evaluation of System Protection Profiles (SPP). Evaluation of SPP is required to demonstrate that an SPP is sound and internally consistent, and, if the SPP is derived from one or more SPPs or packages, that the SPP is a correct instantiation of these SPPs and packages. These properties are necessary for the SPP to be suitable for use as the basis for subsequent STOE evaluation.

The following are the families within this class:

a) ASP_INT: SPP introduction;

b) ASP_CCL: Conformance claims;

c) ASP_SPD: Security problem definition;

d) ASP_OBJ: Security objectives;

e) ASP_ECD: Extended components definition;

f) ASP_REQ: Security requirements;

g) ASP_DMI: Security domain introduction;

h) ASP_DMC: Security domain conformance claims;

i) ASP_DMP: Security domain security problem definition;

j) ASP_DMO: Security domain security objectives;

k) ASP_DMR: Security domain security requirements.

C.2.2 SPP common part

The following specifications apply to the whole SPP. Specifications for specific domains should be described using the domain families (see C.2.9).

C.2.3 SPP introduction (ASP_INT)

C.2.3.1 Objectives

The objective of this family is to describe the STOE in a narrative way.

Evaluation of the SPP introduction is required to demonstrate that the SPP is correctly identified, and that the STOE overview and domain organization specification are consistent with each other. The introductions for specific security domains are defined at C.2.10 security domain introduction.

C.2.3.2 ASP_INT.1 SPP introduction

Dependencies: no dependencies.

C.2.3.2.1 Developer/integrator action elements

ASP_INT.1.1D The developer/integrator shall provide an SPP introduction.

C.2.3.2.2 Content and presentation of evidence elements

ASP_INT.1.1C The SPP introduction shall contain an SPP reference, a STOE overview and a domain organization specification.

ASP_INT.1.2C The SPP reference shall uniquely identify the SPP.

ASP_INT.1.4C The STOE overview shall summarize the usage and major security features of the STOE.

ASP_INT.1.5C The STOE overview shall identify the STOE type.

ASP_INT.1.6C The STOE overview shall identify the relationships and interfaces to any external operational systems required by the STOE.

ASP_INT.1.7C The domain organization specification shall describe the organization of mandated security domains and their identification, physical scope and boundaries of each security domain.

ASP_INT.1.8C For each domain, the domain organization specification shall describe any security services provided by that domain that are to be available to other domains and any security properties of the domain that are to be enforced on other domains.

C.2.3.2.3 Evaluator action elements

ASP_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_INT.1.2E The evaluator shall confirm that the STOE overview and the domain organization specification are consistent with each other.

C.2.4 Conformance claims (ASP_CCL)

C.2.4.1 Objectives

The objective of this family is to determine the validity of various conformance claims: the ISO/IEC 15408 conformance claim, the SPP conformance claim, the PPs conformance claim and the requirements package claim. The ISO/IEC 15408 conformance claim describes the version of ISO/IEC 15408 to which the SPP and STOE claim conformance, the PPs claim (if any) describes how the SPP claims conformance with the identified PPs, the package claim (if any) describes how the SPP claims conformance with the stated package, while the SPP claim identifies the SPPs (if any) that the SPP claims conformance to. Determining the validity of the SPP claim, the PPs claim and the package claim entails determining whether all claimed SPPs, PPs and packages are clearly identified, whether the SPP fully contains these SPPs PPs and packages, and whether all security requirements drawn from these SPPs, PPs and packages are completed correctly. Conformance claims for a specific security domain are defined at C.2.11 security domain conformance claim.

C.2.4.2 ASP_CCL.1 Conformance claims

Dependencies: ASP_INT.1 SPP introduction

ASP_SPD.1 Security problem definition

ASP_OBJ.1 Security objectives

ASP_ECD.1 Extended components definition

ASP_REQ.1 Stated security requirements

C.2.4.2.1 Developer/integrator action elements

ASP_CCL.1.1D The developer/integrator shall provide a conformance claim.

ASP_CCL.1.2D The developer/integrator shall provide a conformance claims rationale.

C.2.4.2.2 Content and presentation of evidence elements

ASP_CCL.1.1C The conformance claim shall contain a criteria conformance claim that identifies the version of ISO/IEC TR 19791 to which the SPP claims conformance.

ASP_CCL.1.2C The criteria conformance claim shall describe the functional conformance of the SPP to ISO/IEC TR 19791 as either ISO/IEC TR 19791 functionally conformant or ISO/IEC TR 19791 functionally extended.

ASP_CCL.1.3C The criteria conformance claim shall describe the assurance conformance of the SPP to ISO/IEC TR 19791 as either ISO/IEC TR 19791 assurance conformant or ISO/IEC 15408 TR 19791 assurance extended.

ASP_CCL.1.4C The criteria conformance claim shall be consistent with the extended components definition.

ASP_CCL.1.5C The conformance claim shall identify all SPPs, PPs and security requirement packages to which the SPP claims conformance.

ASP_CCL.1.6C The conformance claim shall describe any conformance of the SPP to a package as either package-conformant or package-augmented.

ASP_CCL.1.7C The conformance claims rationale shall demonstrate that the STOE type is consistent with the STOE type in the SPPs, PPs and packages for which conformance is being claimed.

ASP_CCL.1.8C The conformance claims rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the SPPs, PPs and packages for which conformance is being claimed.

ASP_CCL.1.9C The conformance claims rationale shall demonstrate that the statement of objectives is consistent with the statement of objectives in the SPPs, PPs and packages for which conformance is being claimed.

ASP_CCL.1.10C The conformance claims rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the SPPs, PPs and packages for which conformance is being claimed.

ASP_CCL.1.11C The conformance claims rationale shall demonstrate that all operations of the security requirements that were taken from a SPP, PP or package are completed consistently with the respective SPP, PP or package.

C.2.4.2.3 Evaluator action elements

ASP_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_CCL.1.2E The evaluator shall confirm that the SPP meets the ISO/IEC 15408 conformance claim.

C.2.5 Security problem definition (ASP_SPD)

C.2.5.1 Objectives

This part of the SPP defines the security problems to be addressed by the STOE, including its development environment. These security problems are applicable to the STOE as a whole. Security problems for a specific security domain are defined at C.2.12 security domain problem definition. Evaluation of the security problem definition is required to demonstrate that the security problems intended to be addressed by the STOE, including its development environment, are clearly defined.

C.2.5.2 ASP_SPD.1 Security problem definition

Dependencies: no dependencies.

C.2.5.2.1 Developer/integrator action elements

ASP_SPD.1.1D The developer/integrator shall provide a security problem definition.

C.2.5.2.2 Content and presentation of evidence elements

ASP_SPD.1.1C The security problem definition shall describe all risks applicable to the STOE. Each risk shall be categorised as acceptable or unacceptable.

ASP_SPD.1.2C All unacceptable risks shall be described in terms of threats and vulnerabilities. Each threat shall be described in terms of a threat agent, an asset, and an adverse action.

ASP_SPD.1.3C The security problem definition shall describe the OSPs.

C.2.5.2.3 Evaluator action elements

ASP_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_SPD.1.2E The evaluator shall confirm that the security problem definition is internally consistent.

C.2.6 Security objectives (ASP_OBJ)

C.2.6.1 Objectives

The security objectives are a concise statement of the intended response to the security problem defined through the ASP_SPD family. The defined security objectives in this part are applicable to the STOE as a whole. Security objectives for a specific security domain are defined at C.2.13 security domain security objectives. Evaluation of the security objectives is required to demonstrate that the security objectives adequately and completely address the security problem definition, that the division of this problem between the STOE, its development environment and external operational systems is clearly defined, and that the security objectives are internally consistent.

C.2.6.2 ASP_OBJ.1 Security objectives

Dependencies: ASP_SPD.1 Security problem definition

C.2.6.2.1 Developer/integrator action elements

ASP_OBJ.1.1D The developer/integrator shall provide a statement of security objectives.

ASP_OBJ.1.2D The developer/integrator shall provide security objectives rationale.

C.2.6.2.2 Content and presentation of evidence elements

ASP_OBJ.1.1C The statement of security objectives shall describe the security objectives for the STOE.

ASP_OBJ.1.2C The statement of security objectives shall describe any security objectives met by external operational systems.

ASP_OBJ.1.3C The statement of security objectives shall describe the security objectives for the development environment.

ASP_OBJ.1.4C The security objectives rationale shall trace each security objective for the STOE back to risks countered by that security objective and OSPs met by that security objective.

ASP_OBJ.1.5C The security objectives rationale shall trace each security objective for external operational systems back to risks countered by that security objective and OSPs met by that security objective.

ASP_OBJ.1.6C The security objectives rationale shall trace each security objective for the development environment back to risks countered by that security objective and OSPs met by that security objective.

ASP_OBJ.1.7C The security objectives rationale shall demonstrate that the security objectives counter all unacceptable risks.

ASP_OBJ.1.8C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

C.2.6.2.3 Evaluator action elements

ASP_OBJ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_OBJ.1.2E The evaluator shall confirm that the statement of security objectives is internally consistent.

C.2.7 Extended components definition (ASP_ECD)

C.2.7.1 Objectives

Extended security requirements are requirements that are not based on components from ISO/IEC 15408 or this Technical Report, but are based on extended components: components defined by the SPP author. Evaluation of the definition of extended components is necessary to determine that they are clear and unambiguous, and that they are necessary, i.e. they could not have been clearly expressed using existing ISO/IEC 15408 or this Technical Report components.

C.2.7.2 ASP_ECD.1 Extended components definition

Dependencies: no dependencies.

C.2.7.2.1 Developer/integrator action elements

ASP_ECD.1.1D The developer/integrator shall provide a statement of security requirements.

ASP_ECD.1.2D The developer/integrator shall provide an extended components definition.

C.2.7.2.2 Content and presentation of evidence elements

ASP_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASP_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASP_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing ISO/IEC 15408 components, families, and classes.

ASP_ECD.1.4C The extended components definition shall use the existing ISO/IEC 15408 components, families, classes, and methodology as a model for presentation.

ASP_ECD.1.5C The extended components shall consist of measurable and objective elements such that compliance or non-compliance to these elements can be demonstrated.

C.2.7.2.3 Evaluator action elements

ASP_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

C.2.8 Security requirements (ASP_REQ)

C.2.8.1 Objectives

The SSFs form a clear and unambiguous description of the expected security behaviour of the STOE. The SSAs form a clear and unambiguous description of the expected activities that will be undertaken to gain assurance in the STOE. The security requirements defined in this part are applicable to the STOE as a whole. Security requirements for a specific security domain are defined at C.2.14 security domain security requirements. Evaluation of the security requirements is required to ensure that they are clear and unambiguous.

C.2.8.2 Component levelling

This family has two components. The components in this family are levelled on whether they are stated as is, or whether they are derived from security objectives for the STOE and its development environment.

C.2.8.3 ASP_REQ.1 Stated security requirements

Dependencies: ASP_ECD.1 Extended components definition

C.2.8.3.1 Developer/integrator action elements

None.

C.2.8.3.2 Content and presentation of evidence elements

ASP_REQ.1.1C The statement of security requirements shall describe the SSFs and the SSAs.

ASP_REQ.1.2C The statement of security requirements shall identify all operations on the security requirements.

ASP_REQ.1.3C All operations shall be performed correctly.

ASP_REQ.1.4C Each dependency between security requirements shall either be satisfied, or identified as "not satisfied".

C.2.8.3.3 Evaluator action elements

ASP_REQ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_REQ.1.2E The evaluator shall confirm that the statement of security requirements is internally consistent.

C.2.8.4 ASP_REQ.2 Derived security requirements

Hierarchical to: ASP_REQ.1 Stated security requirements

Dependencies: ASP_OBJ.1 Security objectives

ASP_ECD.1 Extended components definition

C.2.8.4.1 Developer/integrator action elements

ASP_REQ.2.1D The developer/integrator shall provide a security requirements rationale.

C.2.8.4.2 Content and presentation of evidence elements

ASP_REQ.2.1C The statement of security requirements shall describe the SSFs and the SSAs.

ASP_REQ.2.2C The statement of security requirements shall identify all operations on the security requirements.

ASP_REQ.2.3C All operations shall be performed correctly.

ASP_REQ.2.4C Each dependency between security requirements shall either be satisfied, **or the security requirements rationale shall justify the dependency not being satisfied.**

ASP_REQ.2.5C The security requirements rationale shall trace each SSF back to security objectives for the STOE.

ASP_REQ.2.6C The security requirements rationale shall trace each SSA back to security objectives for the STOE or its development environment.

ASP_REQ.2.7C The security requirements rationale shall demonstrate that the SSFs and SSAs together meet all security objectives for the STOE and its development environment not met by external systems.

C.2.8.4.3 Evaluator action elements

ASP_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_REQ.2.2E The evaluator shall confirm that the statement of security requirements is internally consistent.

C.2.9 SPP security domains

Each SPP security domain defines the security problems, security objectives and security requirements that are unique to that specific security domain.

The following sections define the families that are used to define security domains within the SPP.

C.2.10 Security domain introduction (ASP_DMI)

C.2.10.1 Objectives

The objective of this family is to describe a security domain in a narrative way on three levels of abstraction: security domain reference, security domain overview and security domain description.

C.2.10.2 ASP_DMI.1 Security domain introduction

Dependencies: ASP_INT.1 SPP introduction

C.2.10.2.1 Developer/integrator action elements

ASP_DMI.1.1D The developer/integrator shall provide a security domain introduction.

C.2.10.2.2 Content and presentation of evidence elements

ASP_DMI.1.1C The security domain introduction shall contain a security domain reference, a security domain overview and a security domain description.

ASP_DMI.1.2C The security domain reference shall uniquely identify the security domain.

ASP_DMI.1.3C The security domain overview shall summarize the usage and major security features of the security domain.

ASP_DMI.1.4C The security domain description shall describe the included subsystems and/or components.

ASP_DMI.1.5C The security domain description shall describe the relationships and interfaces to other domains.

C.2.10.2.3 Evaluator action elements

ASP_DMI.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_DMI.1.2E The evaluator shall confirm that the security domain reference, security domain overview and the security domain description are consistent with each other, and with the SPP introduction.

C.2.11 Security domain conformance claims (ASP_DMC)

C.2.11.1 Objectives

This part of the SPP defines the unique conformance claims for a security domain.

C.2.11.2 ASP_DMC.1 Conformance claims

Dependencies: ASP_DMP.1 Security domain security problem definition

ASP_DMO.1 Security domain security objectives

ASP_DMR.1 Stated domain security requirements

C.2.11.2.1 Developer/integrator action elements

ASP_DMC.1.1D The developer/integrator shall provide a domain conformance claim.

ASP_DMC.1.2D The developer/integrator shall provide a domain conformance claims rationale.

C.2.11.2.2 Content and presentation of evidence elements

ASP_DMC.1.1C The domain conformance claim shall identify all SPPs, PPs and security requirement packages to which the domain claims conformance.

ASP_DMC.1.2C The domain conformance claim shall describe any conformance of the domain to a package as either package-conformant or package-augmented.

ASP_DMC.1.3C The domain conformance claims rationale shall demonstrate that the STOE type is consistent with the STOE type in the SPPs, PPs and packages for which conformance is being claimed.

ASP_DMC.1.4C The domain conformance claims rationale shall demonstrate that the statement of the domain security problem definition is consistent with the statement of the security problem definition in the SPPs, PPs and packages for which conformance is being claimed.

ASP_DMC.1.5C The domain conformance claims rationale shall demonstrate that the statement of domain security objectives is consistent with the statement of objectives in the SPPs, PPs and packages for which conformance is being claimed.

ASP_DMC.1.6C The domain conformance claims rationale shall demonstrate that the statement of domain security requirements is consistent with the statement of security requirements in the SPPs, PPs and packages for which conformance is being claimed.

ASP_DMC.1.7C The domain conformance claims rationale shall demonstrate that all operations of the security requirements that were taken from a SPP, PP or package are completed consistently with the respective SPP, PP or package.

C.2.11.2.3 Evaluator action elements

ASP_DMC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.2.12 Security domain security problem definition (ASP_DMP)

C.2.12.1 Objectives

This part of the SPP defines the unique security problems addressed by a security domain.

C.2.12.2 ASP_DMP.1 Security domain security problem definition

Dependencies: no dependencies.

C.2.12.2.1 Developer/integrator action elements

ASP_DMP.1.1D The developer/integrator shall provide a domain security problem definition.

C.2.12.2.2 Content and presentation of evidence elements

ASP_DMP.1.1C The domain security problem definition shall describe all unique risks applicable to the domain. Each risk shall be categorised as acceptable or unacceptable.

ASP_DMP.1.2C All unacceptable risks shall be described in terms of threats and vulnerabilities. Each threat shall be described in terms of a threat agent, an asset, and an adverse action.

ASP_DMP.1.3C The domain security problem definition shall describe the unique OSPs applicable to the domain.

C.2.12.2.3 Evaluator action elements

ASP_DMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_DMP.1.2E The evaluator shall confirm that the domain security problem definition is internally consistent.

C.2.13 Security domain security objectives (ASP_DMO)

C.2.13.1 Objectives

This part of the SPP specifies a concise statement of the intended response to the unique security problems defined through the ASP_DMP family.

C.2.13.2 ASP_DMO.1 Security domain security objectives

Dependencies: ASP_INT.1 SPP introduction

ASP_DMP.1 Security domain security problem definition

C.2.13.2.1 Developer/integrator action elements

ASP_DMO.1.1D The developer/integrator shall provide a statement of domain security objectives.

ASP_DMO.1.2D The developer/integrator shall provide a domain security objectives rationale.

C.2.13.2.2 Content and presentation of evidence elements

ASP_DMO.1.1C The statement of domain security objectives shall describe the unique security objectives for the domain.

ASP_DMO.1.2C The statement of domain security objectives shall describe any security objectives for the domain that are met by other domains or external operational systems.

ASP_DMO.1.3C The statement of domain security objectives shall describe any security objectives for the domain that are enforced on or available to other domains.

ASP_DMO.1.4C The statement of domain security objectives shall describe the unique security objectives for the domain development environment.

ASP_DMO.1.5C The domain security objectives rationale shall trace each unique security objective for the domain back to risks countered by that security objective and OSPs met by that security objective.

ASP_DMO.1.6C The domain security objectives rationale shall trace each unique security objective for the domain development environment back to risks countered by that security objective and OSPs met by that security objective.

ASP_DMO.1.7C The domain security objectives rationale shall trace each unique security objective for other domains back to risks countered by that security objective and OSPs met by that security objective.

ASP_DMO.1.8C The domain security objectives rationale shall demonstrate that the security objectives counter all unique unacceptable risks to the domain.

ASP_DMO.1.9C The domain security objectives rationale shall demonstrate that the security objectives enforce all unique OSPs for the domain.

C.2.13.2.3 Evaluator action elements

ASP_DMO.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_DMO.1.2E The evaluator shall confirm that the statement of domain security objectives is internally consistent.

ASP_DMO.1.3E The evaluator shall confirm that the statement of domain security objectives is consistent with the domain organization specification.

C.2.14 Security domain security requirements (ASP_DMR)

C.2.14.1 Objectives

This part of the SPP provides a clear and unambiguous description of the expected unique security behaviour of the security domain.

C.2.14.2 Component levelling

This family has two components. The components in this family are levelled on whether they are stated as is, or whether they are derived from security objectives for the domain and its development environment.

C.2.14.3 ASP_DMR.1 Stated domain security requirements

Dependencies: ASP_ECD.1 Extended components definition

C.2.14.3.1 Developer/integrator action elements

None.

C.2.14.3.2 Content and presentation of evidence elements

ASP_DMR.1.1C The statement of domain security requirements shall describe the unique SSFs and SSAs applicable to the domain.

ASP_DMR.1.2C The statement of domain security requirements shall identify all operations on the security requirements.

ASP_DMR.1.3C All operations shall be performed correctly.

ASP_DMR.1.4C Each dependency between domain security requirements shall either be satisfied, or identified as "not satisfied".

C.2.14.3.3 Evaluator action elements

ASP_DMR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_DMR.1.2E The evaluator shall confirm that the statement of domain security requirements is internally consistent.

C.2.14.4 ASP_DMR.2 Derived domain security requirements

Hierarchical to: ASP_DMR.1 Stated domain security requirements

Dependencies: ASP_DMO.1 Security domain security objectives

ASP_ECD.1 Extended components definition

C.2.14.4.1 Developer/integrator action elements

ASP_DMR.2.1D The developer/integrator shall provide a domain security requirements rationale.

C.2.14.4.2 Content and presentation of evidence elements

ASP_DMR.2.1C The statement of domain security requirements shall describe the unique SSFs and SSAs applicable to the domain.

ASP_DMR.2.2C The statement of domain security requirements shall identify all operations on the security requirements.

ASP_DMR.2.3C All operations shall be performed correctly.

ASP_DMR.2.4C Each dependency between domain security requirements shall either be satisfied, **or the domain security requirements rationale shall justify the dependency not being satisfied.**

ASP_DMR.2.5C The domain security requirements rationale shall trace each domain SSF back to the security objectives for the domain.

ASP_DMR.2.6C The domain security requirements rationale shall trace each domain SSA back to the security objectives for the domain or its development environment.

ASP_DMR.2.7C The domain security requirements rationale shall demonstrate that the domain SSFs and SSAs meet all unique security objectives for the domain and its development environment not met by other domains or external systems.

C.2.14.4.3 Evaluator action elements

ASP_DMR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASP_DMR.2.2E The evaluator shall confirm that the statement of domain security requirements is internally consistent.

C.3 Class ASS: System Security Target evaluation

C.3.1 Introduction

This clause provides assurance criteria for the evaluation of System Security Targets (SST). Evaluation of an SST is required to demonstrate that the SST is sound and internally consistent, and, if the SST is based on one or more SPPs or packages, that the SST is a correct instantiation of these SPPs and packages. These properties are necessary for the SST to be suitable for use as the basis for the rest of the STOE evaluation.

The following are the families within this class:

a) ASS_INT: SST introduction;

b) ASS_CCL: Conformance claims;

c) ASS_SPD: Security problem definition;

d) ASS_OBJ: Security objectives;

e) ASS_ECD: Extended components definition;

f) ASS_REQ: Security requirements;

g) ASS_TSS: STOE summary specification;

h) ASS_DMI: Security domain introduction;

i) ASS_DMC: Security domain conformance claims;

j) ASS_DMP: Security domain security problem definition;

k) ASS_DMO: Security domain security objectives;

l) ASS_DMR: Security domain security requirements.

C.3.2 SST common part

The following specifications apply to the whole SST. Specifications for specific domains should be described using the domain families (see C.3.10).

C.3.3 SST introduction (ASS_INT)

C.3.3.1 Objectives

The objective of this family is to describe the STOE in a narrative way on four levels of abstraction: SST/STOE reference, STOE overview, STOE description, and domain organization.

Evaluation of the SST introduction is required to demonstrate that the SST and the STOE are correctly identified, that the STOE is correctly described at four levels of abstraction and that these four descriptions are consistent with each other. The introductions for specific security domains are defined at C.3.11 security domain introduction.

C.3.3.2 ASS_INT.1 SST introduction

Dependencies: no dependencies.

C.3.3.2.1 Developer/integrator action elements

ASS_INT.1.1D The developer/integrator shall provide an SST introduction.

C.3.3.2.2 Content and presentation of evidence elements

ASS_INT.1.1C The SST introduction shall contain an SST reference, a STOE reference, a STOE overview, a STOE description and a domain organization specification.

ASS_INT.1.2C The SST reference shall uniquely identify the SST.

ASS_INT.1.3C The STOE reference shall identify the STOE.

ASS_INT.1.4C The STOE overview shall summarize the usage and major security features of the STOE.

ASS_INT.1.5C The STOE overview shall identify the STOE type.

ASS_INT.1.6C The STOE overview shall identify the relationships and interfaces to any external operational systems required by the STOE.

ASS_INT.1.7C The STOE description shall describe the physical scope and boundaries of the STOE.

ASS_INT.1.8C The STOE description shall describe the logical scope and boundaries of the STOE.

ASS_INT.1.9C The STOE description shall describe the development environments for the STOE, including any unique characteristics of individual domain development environments.

ASS_INT.1.10C The domain organization specification shall describe the organization of constructed security domains and the identification, physical scope and boundaries of each security domain.

ASS_INT.1.11C For each domain, the domain organization specification shall describe any security services provided by that domain that are available to other domains and any security properties of the domain that are enforced on other domains.

C.3.3.2.3 Evaluator action elements

ASS_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_INT.1.2E The evaluator shall confirm that the STOE reference, the STOE overview, the STOE description and the domain organization specification are consistent with each other.

C.3.4 Conformance claims (ASS_CCL)

C.3.4.1 Objectives

The objective of this family is to determine the validity of various conformance claims: the ISO/IEC 15408 conformance claim, the SPP claim, the PPs claim, the STs claim and the requirements package claim. The ISO/IEC 15408 conformance claim describes the version of ISO/IEC 15408 to which the SPP and STOE claim conformance, the PPs, STs and/or package claim (if any) describes how the SST claims conformance with the stated PPs, STs and/or package, while the SPP claim identifies the SPPs (if any) that the SST claims conformance to. Determining the validity of the SPP claim, the PPs claim, the STs claim and the package claim entails determining whether all claimed SPPs, PPs, STs and packages are clearly identified, whether the SST fully contains these SPPs, PPs, STs and packages, and whether all security requirements drawn from these SPPs, PPs, STs and packages are completed correctly. Conformance claims for a specific security domain are defined at C.3.12 security domain conformance claim.

C.3.4.2 ASS_CCL.1 Conformance claims

Dependencies: ASS_INT.1 SST introduction

ASS_SPD.1 Security problem definition

ASS_OBJ.1 Security objectives

ASS_ECD.1 Extended components definition

ASS_REQ.1 Stated security requirements

C.3.4.2.1 Developer/integrator action elements

ASS_CCL.1.1D The developer/integrator shall provide a conformance claim.

ASS_CCL.1.2D The developer/integrator shall provide a conformance claims rationale.

C.3.4.2.2 Content and presentation of evidence elements

ASS_CCL.1.1C The conformance claim shall contain a criteria conformance claim that identifies the version of ISO/IEC TR 19791 to which the SST and the STOE claim conformance.

ASS_CCL.1.2C The criteria conformance claim shall describe the functional conformance of the SST to ISO/IEC TR 19791 as either ISO/IEC TR 19791 functionally conformant or ISO/IEC TR 19791 functionally extended.

ASS_CCL.1.3C The criteria conformance claim shall describe the assurance conformance of the SST to ISO/IEC TR 19791 as either ISO/IEC TR 19791 assurance conformant or ISO/IEC TR 19791 assurance extended.

ASS_CCL.1.4C The criteria conformance claim shall be consistent with the extended components definition.

ASS_CCL.1.5C The conformance claim shall identify all SPPs, PPs, STs and security requirement packages to which the SST claims conformance.

ASS_CCL.1.6C The conformance claim shall describe any conformance of the SST to a package as either package-conformant or package-augmented.

ASS_CCL.1.7C The conformance claims rationale shall demonstrate that the STOE type is consistent with the STOE type in the SPPs, PPs, STs and packages for which conformance is being claimed.

ASS_CCL.1.8C The conformance claims rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the SPPs, PPs, STs and packages for which conformance is being claimed.

ASS_CCL.1.9C The conformance claims rationale shall demonstrate that the statement of objectives is consistent with the statement of objectives in the SPPs, PPs, STs and packages for which conformance is being claimed.

ASS_CCL.1.10C The conformance claims rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the SPPs, PPs, STs and packages for which conformance is being claimed.

ASS_CCL.1.11C The conformance claims rationale shall demonstrate that all operations of the security requirements that were taken from a SPP, PP, ST or package are completed consistently with the respective SPP, PP, ST or package.

C.3.4.2.3 Evaluator action elements

ASS_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_CCL.1.2E The evaluator shall confirm that the SST meets the ISO/IEC 15408 conformance claim.

C.3.5 Security problem definition (ASS_SPD)

C.3.5.1 Objectives

This part of the SST defines the security problems to be addressed by the STOE, including its development environment. These security problems are applicable to the STOE as a whole. Security problems for a specific security domain are defined at C.3.13 security domain security problem definition. Evaluation of the security problem definition is required to demonstrate that the security problems intended to be addressed by the STOE, including its development environment, are clearly defined.

C.3.5.2 ASS_SPD.1 Security problem definition

Dependencies: no dependencies.

C.3.5.2.1 Developer/integrator action elements

ASS_SPD.1.1D The developer/integrator shall provide a security problem definition.

C.3.5.2.2 Content and presentation of evidence elements

ASS_SPD.1.1C The security problem definition shall describe all risks applicable to the STOE. Each risk shall be categorised as acceptable or unacceptable.

ASS_SPD.1.2C All unacceptable risks shall be described in terms of threats and vulnerabilities. Each threat shall be described in terms of a threat agent, an asset, and an adverse action.

ASS_SPD.1.3C The security problem definition shall describe the OSPs.

C.3.5.2.3 Evaluator action elements

ASS_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_SPD.1.2E The evaluator shall confirm that the security problem definition is internally consistent.

C.3.6 Security objectives (ASS_OBJ)

C.3.6.1 Objectives

The security objectives are a concise statement of the intended response to the security problem defined through the ASS_SPD family. The defined security objectives in this part are applicable to the STOE as a whole. Security objectives for a specific security domain are defined at C.3.14 security domain security objectives. Evaluation of the security objectives is required to demonstrate that the security objectives adequately and completely address the security problem definition, that the division of this problem between the STOE, its development environment and external operational systems is clearly defined, and that the security objectives are internally consistent.

C.3.6.2 ASS_OBJ.1 Security objectives

Dependencies: ASS_SPD.1 Security problem definition

C.3.6.2.1 Developer/integrator action elements

ASS_OBJ.1.1D The developer/integrator shall provide a statement of security objectives.

ASS_OBJ.1.2D The developer/integrator shall provide security objectives rationale.

C.3.6.2.2 Content and presentation of evidence elements

ASS_OBJ.1.1C The statement of security objectives shall describe the security objectives for the STOE.

ASS_OBJ.1.2C The statement of security objectives shall describe any security objectives met by external operational systems.

ASS_OBJ.1.3C The statement of security objectives shall describe the security objectives for the development environment.

ASS_OBJ.1.4C The security objectives rationale shall trace each security objective for the STOE back to risks countered by that security objective and OSPs met by that security objective.

ASS_OBJ.1.5C The security objectives rationale shall trace each security objective for external operational systems back to risks countered by that security objective and OSPs met by that security objective.

ASS_OBJ.1.6C The security objectives rationale shall trace each security objective for the development environment back to risks countered by that security objective and OSPs met by that security objective.

ASS_OBJ.1.7C The security objectives rationale shall demonstrate that the security objectives counter all unacceptable risks.

ASS_OBJ.1.8C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

C.3.6.2.3 Evaluator action elements

ASS_OBJ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_OBJ.1.2E The evaluator shall confirm that the statement of security objectives is internally consistent.

C.3.7 Extended components definition (ASS_ECD)

C.3.7.1 Objectives

Extended security requirements are requirements that are not based on components from ISO/IEC 15408 or this Technical Report, but are based on extended components: components defined by the SST author. Evaluation of the definition of extended components is necessary to determine that they are clear and unambiguous, and that they are necessary, i.e. they could not have been clearly expressed using existing ISO/IEC 15408 or this Technical Report components.

C.3.7.2 ASS_ECD.1 Extended components definition

Dependencies: no dependencies.

C.3.7.3 Developer/integrator action elements

ASS_ECD.1.1D The developer/integrator shall provide a statement of security requirements.

ASS_ECD.1.2D The developer/integrator shall provide an extended components definition.

C.3.7.3.1 Content and presentation of evidence elements

ASS_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASS_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASS_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing ISO/IEC 15408 components, families, and classes.

ASS_ECD.1.4C The extended components definition shall use the existing ISO/IEC 15408 components, families, classes, and methodology as a model for presentation.

ASS_ECD.1.5C The extended components shall consist of measurable and objective elements such that compliance or non-compliance to these elements can be demonstrated.

C.3.7.3.2 Evaluator action elements

ASS_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

C.3.8 Security requirements (ASS_REQ)

C.3.8.1 Objectives

The SSFs form a clear and unambiguous description of the expected security behaviour of the STOE. The SSAs form a clear and unambiguous description of the expected activities that will be undertaken to gain assurance in the STOE. The security requirements defined in this part are applicable to the STOE as a whole. Security requirements for a specific security domain are defined at C.3.15 security domain security requirements. Evaluation of the security requirements is required to ensure that they are clear and unambiguous.

C.3.8.2 Component levelling

This family has two components. The components in this family are levelled on whether they are stated as is, or whether they are derived from security objectives for the STOE and its development environment.

C.3.8.3 ASS_REQ.1 Stated security requirements

Dependencies: ASS_ECD.1 Extended components definition

C.3.8.3.1 Developer/integrator action elements

None.

C.3.8.3.2 Content and presentation of evidence elements

ASS_REQ.1.1C The statement of security requirements shall describe the SSFs and the SSAs.

ASS_REQ.1.2C The statement of security requirements shall identify all operations on the security requirements.

ASS_REQ.1.3C All assignment and selection operations shall be completed.

ASS_REQ.1.4C All operations shall be performed correctly.

ASS_REQ.1.5C Each dependency between security requirements shall either be satisfied, or identified as "not satisfied".

C.3.8.3.3 Evaluator action elements

ASS_REQ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_REQ.1.2E The evaluator shall confirm that the statement of security requirements is internally consistent.

C.3.8.4 ASS_REQ.2 Derived security requirements

Hierarchical to: ASS_REQ.1 Stated security requirements

Dependencies: ASS_OBJ.1 Security objectives

ASS_ECD.1 Extended components definition

C.3.8.4.1 Developer/integrator action elements

ASS_REQ.2.1D The developer/integrator shall provide a security requirements rationale.

C.3.8.4.2 Content and presentation of evidence elements

ASS_REQ.2.1C The statement of security requirements shall describe the SSFs and the SSAs.

ASS_REQ.2.2C The statement of security requirements shall identify all operations on the security requirements.

ASS_REQ.2.3C All assignment and selection operations shall be completed.

ASS_REQ.2.4C All operations shall be performed correctly.

ASS_REQ.2.5C Each dependency between security requirements shall either be satisfied, **or the security requirements rationale shall justify the dependency not being satisfied.**

ASS_REQ.2.6C The security requirements rationale shall trace each SSF back to security objectives for the STOE.

ASS_REQ.2.7C The security requirements rationale shall trace each SSA back to security objectives for the STOE or its development environment.

ASS_REQ.2.8C The security requirements rationale shall demonstrate that the SSFs and SSAs together meet all security objectives for the STOE and its development environment not met by external systems.

C.3.8.4.3 Evaluator action elements

ASS_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_REQ.2.2E The evaluator shall confirm that the statement of security requirements is internally consistent.

C.3.9 STOE summary specification (ASS_TSS)

C.3.9.1 Objectives

The objective for the STOE summary specification is to provide potential consumers of the STOE with a high-level description of how the developer/integrator intends to satisfy its SSFs and SSAs. The STOE summary specification should allow evaluators and potential consumers to understand how the STOE meets its SSFs and SSAs. The STOE summary specification defined in this part is applicable to the STOE as a whole. The security summary specification for a specific security domain is defined at C.3.16 STOE security domain summary specification. Evaluation of the STOE summary specification is necessary to determine whether all SSFs have been adequately addressed, and whether the STOE summary specification is consistent with other narrative descriptions of the STOE.

C.3.9.2 ASS_TSS.1 STOE summary specification

Dependencies: ASS_INT.1 SST introduction

ASS_REQ.1 Stated security requirements

C.3.9.2.1 Developer/integrator action elements

ASS_TSS.1.1D The developer/integrator shall provide a STOE summary specification.

C.3.9.2.2 Content and presentation of evidence elements

ASS_TSS.1.1C The STOE summary specification shall describe how the STOE meets each SSF.

ASS_TSS.1.2C The STOE summary specification shall describe how the STOE and its development environment meets each SSA.

C.3.9.2.3 Evaluator action elements

ASS_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_TSS.1.2E The evaluator shall confirm that the STOE summary specification is consistent with the STOE overview and the STOE description.

C.3.10 STOE Security domains

Each STOE security domain defines the security problems, security objectives and security requirements that are unique to that specific security domain.

The following sections define the families that are used to define security domains within the STOE.

C.3.11 Security domain introduction (ASS_DMI)

C.3.11.1 Objectives

The objective of this family is to describe a security domain in a narrative way on three levels of abstraction: security domain reference, security domain overview and security domain description.

C.3.11.2 ASS_DMI.1 Security domain introduction

Dependencies: ASS_INT.1 SST introduction.

C.3.11.2.1 Developer/integrator action elements

ASS_DMI.1.1D The developer/integrator shall provide a security domain introduction.

C.3.11.2.2 Content and presentation of evidence elements

ASS_DMI.1.1C The security domain introduction shall contain a security domain reference, a security domain overview and a security domain description.

ASS_DMI.1.2C The security domain reference shall uniquely identify the security domain.

ASS_DMI.1.3C The security domain overview shall summarize the usage and major security features of the security domain.

ASS_DMI.1.4C The security domain description shall describe the included subsystems and/or components.

ASS_DMI.1.5C The security domain description shall describe the relationships and interfaces to other domains.

C.3.11.2.3 Evaluator action elements

ASS_DMI.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_DMI.1.2E The evaluator shall confirm that the security domain reference, security domain overview and the security domain description are consistent with each other, and with the SST introduction.

C.3.12 Security domain conformance claims (ASS_DMC)

C.3.12.1 Objectives

This part of the SST defines the specific conformance claim for the security domain.

C.3.12.2 ASS_DMC.1 Conformance claims

Dependencies: ASS_DMP.1 Security domain security problem definition

ASS_DMO.1 Security domain security objectives

ASS_DMR.1 Stated domain security requirements

C.3.12.2.1 Developer/integrator action elements

ASS_DMC.1.1D The developer/integrator shall provide a domain conformance claim.

ASS_DMC.1.2D The developer/integrator shall provide a domain conformance claims rationale.

C.3.12.2.2 Content and presentation of evidence elements

ASS_DMC.1.1C The domain conformance claim shall identify all SPPs, PPs, STs and security requirement packages to which the domain claims conformance.

ASS_DMC.1.2C The domain conformance claim shall describe any conformance of the domain to a package as either package-conformant or package-augmented.

ASS_DMC.1.3C The domain conformance claims rationale shall demonstrate that the STOE type is consistent with the STOE type in the SPPs, PPs, STs and packages for which conformance is being claimed.

ASS_DMC.1.4C The domain conformance claims rationale shall demonstrate that the statement of the domain security problem definition is consistent with the statement of the security problem definition in the SPPs, PPs, STs and packages for which conformance is being claimed.

ASS_DMC.1.5C The domain conformance claims rationale shall demonstrate that the statement of domain security objectives is consistent with the statement of objectives in the SPPs, PPs, STs and packages for which conformance is being claimed.

ASS_DMC.1.6C The domain conformance claims rationale shall demonstrate that the statement of domain security requirements is consistent with the statement of security requirements in the SPPs, PPs, STs and packages for which conformance is being claimed.

ASS_DMC.1.7C The domain conformance claims rationale shall demonstrate that all operations of the security requirements that were taken from a SPP, PP, ST or package are completed consistently with the respective SPP, PP, ST or package.

C.3.12.2.3 Evaluator action elements

ASS_DMC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.3.13 Security domain security problem definition (ASS_DMP)

C.3.13.1 Objectives

This part of the SST defines the specific security problems addressed by a security domain.

C.3.13.2 ASS_DMP.1 Security domain security problem definition

Dependencies: no dependencies.

C.3.13.2.1 Developer/integrator action elements

ASS_DMP.1.1D The developer/integrator shall provide a domain security problem definition.

C.3.13.2.2 Content and presentation of evidence elements

ASS_DMP.1.1C The domain security problem definition shall describe all unique risks applicable to the domain. Each risk shall be categorised as acceptable or unacceptable.

ASS_DMP.1.2C All unacceptable risks shall be described in terms of threats and vulnerabilities. Each threat shall be described in terms of a threat agent, an asset, and an adverse action.

ASS_DMP.1.3C The domain security problem definition shall describe the unique OSPs applicable to the domain.

C.3.13.2.3 Evaluator action elements

ASS_DMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_DMP.1.2E The evaluator shall confirm that the domain security problem definition is internally consistent.

C.3.14 Security domain security objectives (ASS_DMO)

C.3.14.1 Objectives

This part of the SST specifies a concise statement of the intended response to the unique domain security problems defined through the ASS_DMP family.

C.3.14.2 ASS_DMO.1 Security domain security objectives

Dependencies: ASS_INT.1 SST introduction

ASS_DMP.1 Security domain security problem definition

C.3.14.2.1 Developer/integrator action elements

ASS_DMO.1.1D The developer/integrator shall provide a statement of domain security objectives.

ASS_DMO.1.2D The developer/integrator shall provide a domain security objectives rationale.

C.3.14.2.2 Content and presentation of evidence elements

ASS_DMO.1.1C The statement of domain security objectives shall describe the unique security objectives for the domain.

ASS_DMO.1.2C The statement of domain security objectives shall describe any security objectives for the domain that are met by other domains or external operational systems.

ASS_DMO.1.3C The statement of domain security objectives shall describe any security objectives for the domain that are enforced on or available to other domains.

ASS_DMO.1.4C The statement of domain security objectives shall describe the unique security objectives for the domain development environment.

ASS_DMO.1.5C The domain security objectives rationale shall trace each unique security objective for the domain back to risks countered by that security objective and OSPs met by that security objective.

ASS_DMO.1.6C The domain security objectives rationale shall trace each unique security objective for the domain development environment back to risks countered by that security objective and OSPs met by that security objective.

ASS_DMO.1.7C The domain security objectives rationale shall trace each unique security objective for other domains back to risks countered by that security objective and OSPs met by that security objective.

ASS_DMO.1.8C The domain security objectives rationale shall demonstrate that the security objectives counter all unacceptable risks unique to the domain.

ASS_DMO.1.9C The domain security objectives rationale shall demonstrate that the security objectives enforce all unique OSPs for the domain.

C.3.14.2.3 Evaluator action elements

ASS_DMO.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_DMO.1.2E The evaluator shall confirm that the statement of domain security objectives is internally consistent.

ASS_DMO.1.3E The evaluator shall confirm that the statement of domain security objectives is consistent with the domain organization specification.

C.3.15 Security domain security requirements (ASS_DMR)

C.3.15.1 Objectives

This part of the SST provides a clear and unambiguous description of the expected unique security behaviour of the security domain.

C.3.15.2 Component levelling

This family has two components. The components in this family are levelled on whether they are stated as is, or whether they are derived from security objectives for the domain and its development environment.

C.3.15.3 ASS_DMR.1 Stated domain security requirements

Dependencies: ASS_ECD.1 Extended components definition

C.3.15.3.1 Developer/integrator action elements

None.

C.3.15.3.2 Content and presentation of evidence elements

ASS_DMR.1.1C The statement of domain security requirements shall describe the unique SSFs and SSAs applicable to the domain.

ASS_DMR.1.2C The statement of domain security requirements shall identify all operations on the security requirements.

ASS_DMR.1.3C All assignment and selection operations shall be completed.

ASS_DMR.1.4C All operations shall be performed correctly.

ASS_DMR.1.5C Each dependency between domain security requirements shall either be satisfied, or identified as "not satisfied".

C.3.15.3.3 Evaluator action elements

ASS_DMR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_DMR.1.2E The evaluator shall confirm that the statement of domain security requirements is internally consistent.

C.3.15.4 ASS_DMR.2 Derived domain security requirements

Hierarchical to: ASS_DMR.1 Stated domain security requirements

Dependencies: ASS_DMO.1 Security domain security objectives

ASS_ECD.1 Extended components definition

C.3.15.4.1 Developer/integrator action elements

ASS_DMR.2.1D The developer/integrator shall provide a domain security requirements rationale.

C.3.15.4.2 Content and presentation of evidence elements

ASS_DMR.2.1C The statement of domain security requirements shall describe the unique SSFs and SSAs applicable to the domain.

ASS_DMR.2.2C The statement of domain security requirements shall identify all operations on the security requirements.

ASS_DMR.2.3C All assignment and selection operations shall be completed.

ASS_DMR.2.4C All operations shall be performed correctly.

ASS_DMR.2.5C Each dependency between domain security requirements shall either be satisfied, **or the domain security requirements rationale shall justify the dependency not being satisfied.**

ASS_DMR.2.6C The domain security requirements rationale shall trace each domain SSF back to the security objectives for the domain.

ASS_DMR.2.7C The domain security requirements rationale shall trace each domain SSA back to the security objectives for the domain or its development environment.

ASS_DMR.2.8C The domain security requirements rationale shall demonstrate that the domain SSFs and SSAs meet all unique security objectives for the domain and its development environment not met by other domains or external systems.

C.3.15.4.3 Evaluator action elements

ASS_DMR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_DMR.2.2E The evaluator shall confirm that the statement of domain security requirements is internally consistent.

C.3.16 Security domain summary specification (ASS_DMS)

C.3.16.1 Objectives

This part of the SST specifies the security domain summary specification.

C.3.16.2 ASS_DMS.1 Security domain summary specification

Dependencies: ASS_DMI.1 Security domain introduction

ASS_DMR.1 Stated domain security requirements

C.3.16.2.1 Developer/integrator action elements

ASS_DMS.1.1D The developer/integrator shall provide a domain summary specification.

C.3.16.2.2 Content and presentation of evidence elements

ASS_DMS.1.1C The domain summary specification shall describe how the domain meets each domain SSF.

ASS_DMS.1.2C The domain summary specification shall describe how the domain and its development environment meets each domain SSA.

C.3.16.2.3 Evaluator action elements

ASS_DMS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASS_DMS.1.2E The evaluator shall confirm that the domain summary specification is consistent with the domain overview and the domain description.

C.4 Class AOD: Operational system guidance document

C.4.1 Introduction

The purpose of the operational system guidance document class is to judge the adequacy of the documentation describing the integration and operational use of the operational system. Such documentation includes that aimed at operational system integrators, trusted administrators and non-administrator users whose incorrect actions could adversely affect the security behaviour and characteristics of the operational

system, as well as that aimed at normal users whose incorrect actions could adversely affect the ability of the operational system to provide the required protection capabilities for their own data.

Therefore, the AOD activity is closely related to the processes and procedures defined by the operational security requirements. The user and administrator guidance includes information regarding the technology aspects of the operational system as well as the operational and human processes of the operational system.

C.4.2 Application Notes

All OSF requirements defined in the SST as they apply to required personnel behaviour should be described in the appropriate operational system guidance document.

Maintenance mode, single user mode and any special mode of operation entered following an error or exception should be identified and considered for their consequences and implication for maintaining secure operation.

Administrator guidance should identify the following information:

— the functions and privileges that must be controlled

— the types of controls required for them

— the reasons for such controls.

Warnings should cover expected effects, possible side effects and possible interactions with other functions and privileges.

The guidance should describe the administration of the operational system as a whole, in addition to that for individual products and sub-systems. Administrator guidance that is not only for application programs but also for the whole operational system should be documented.

C.4.3 Operational System Configuration Specification (AOD_OCD)

C.4.3.1 Objectives

The purpose of the operational system configuration specification is to specify the security relevant configuration parameters that support the integration of the operational system components and that allow the operational system security functions to implement and enforce the operational system security concept of operation and associated policies.

C.4.3.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.4.3.3 AOD_OCD.1 Operational system configuration specification

Dependencies: ASD_CON.1 Security concept of operations

ASD_CMP.1 Component design

C.4.3.3.1 Developer/integrator action elements

AOD_OCD.1.1D The developer/integrator shall provide a configuration specification that defines the security relevant configuration parameters that support the integration of the system components and that allow the system security functions to implement and enforce the system security concept of operations and associated policies.

C.4.3.3.2 Content and presentation of evidence elements

AOD_OCD.1.1C The configuration specification shall describe all configuration requirements relative to the STOE including its operational environment.

AOD_OCD.1.2C The configuration specification shall describe the security configuration parameters available to the system integrator or equivalent users/administrators of the STOE with that role and responsibility.

AOD_OCD.1.3C The configuration specification shall describe the use of security parameters configurable by the STOE to implement and enforce the system security policies.

AOD_OCD.1.4C The configuration specification shall contain warnings about configuration accessible functions and privileges that should be controlled in a secure processing environment.

AOD_OCD.1.5C The configuration specification shall clearly present all configuration related responsibilities necessary for secure operation of the STOE.

AOD_OCD.1.6C The configuration specification shall be consistent with all other documentation supplied for evaluation.

AOD_OCD.1.7C The configuration specification shall show that all component security parameters required by the security concept of operations are implemented by the component design.

C.4.3.3.3 Evaluator action elements

AOD_OCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.4.3.4 AOD_OCD.2 Operational system configuration specification verification

Hierarchical to: AOD_OCD.1 Operational system configuration specification

Dependencies: ASD_CON.1 Security concept of operations

ASD_CMP.1 Component design

C.4.3.4.1 Developer/integrator action elements

AOD_OCD.2.1D The developer/integrator shall provide a configuration specification that defines the security relevant configuration parameters that support the integration of the system components and that allow the system security functions to implement and enforce the system security concept of operations and associated policies.

C.4.3.4.2 Content and presentation of evidence elements

AOD_OCD.2.1C The configuration specification shall describe all configuration requirements relative to the STOE including its operational environment.

AOD_OCD.2.2C The configuration specification shall describe the security configuration parameters available to the system integrator or equivalent users/administrators of the STOE with that role and responsibility.

AOD_OCD.2.3C The configuration specification shall describe the use of security parameters configurable by the STOE to implement and enforce the system security policies.

AOD_OCD.2.4C The configuration specification shall contain warnings about configuration accessible functions and privileges that should be controlled in a secure processing environment.

AOD_OCD.2.5C The configuration specification shall clearly present all configuration related responsibilities necessary for secure operation of the STOE.

AOD_OCD.2.6C The configuration specification shall be consistent with all other documentation supplied for evaluation.

AOD_OCD.2.7C The configuration specification shall show that all component security parameters required by the security concept of operations are implemented by the component design.

C.4.3.4.3 Evaluator action elements

AOD_OCD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOD_OCD.2.2E The evaluator shall independently verify the practice of the configuration parameter defined in the configuration specification.

C.4.4 Administrator guidance for an operational system (AOD_ADM)

C.4.4.1 Objectives

Administrator guidance for an operational system is intended to be used by those persons responsible for configuring, maintaining, and administering the STOE in a correct manner for security controls. Security policy, procedures, rules, responsibility and other security requirements that are defined by operational requirements and are intended to be used by administrator should also be described in the administrator guidance. Administrator guidance for an operational system is intended to help administrators understand the security controls provided by the STOE, including both technical and operational controls that require the administrator to perform security-critical actions and those functions that provide security-critical information.

C.4.4.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.4.4.3 Application notes

The content of the administrator guidance documentation will directly be reflected by the policies, rules, responsibilities, procedures and operational security measures that are related with the administrator and are defined in the operational controls. The requirements AOD_ADM.1.3C and AOD_ADM.1.7C encompass the aspect that any warnings to the users of a STOE with regard to the STOE security environment and the security objectives described in the SPP/SST are appropriately covered in the administrator guidance.

The concept of secure values, as employed in AOD_ADM.1.6C, has relevance where an administrator has control over security parameters. Guidance needs to be provided on secure and insecure settings for such parameters.

C.4.4.4 AOD_ADM.1 Administrator guidance

Dependencies: ASD_SAD.1 Architecture description

C.4.4.4.1 Management action elements

AOD_ADM.1.1M The management shall provide administrator guidance for the operational system addressed to system administrative personnel.

C.4.4.4.2 Content and presentation of evidence elements

AOD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the STOE.

AOD_ADM.1.2C The administrator guidance shall describe the operational control requirements correctly that are related to the administrator.

AOD_ADM.1.3C The administrator guidance shall describe how to administer the STOE in a secure manner.

AOD_ADM.1.4C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AOD_ADM.1.5C The administrator guidance shall describe all operations regarding user behaviour that are relevant to secure operation of the STOE.

AOD_ADM.1.6C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AOD_ADM.1.7C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the SSF.

AOD_ADM.1.8C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AOD_ADM.1.9C The administrator guidance shall describe all interfaces to external operational systems that are relevant to the administrator.

C.4.4.4.3 Evaluator action elements

AOD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.4.4.5 AOD_ADM.2 Administrator guidance verification

Hierarchical to: AOD_ADM.1 Administrator guidance

Dependencies: ASD_SAD.1 Architecture description

C.4.4.5.1 Management action elements

AOD_ADM.2.1M The management shall provide administrator guidance for the operational system addressed to system administrative personnel.

C.4.4.5.2 Content and presentation of evidence elements

AOD_ADM.2.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the STOE.

AOD_ADM.1.2C The administrator guidance shall describe the operational control requirements correctly that are related to the administrator.

AOD_ADM.2.3C The administrator guidance shall describe how to administer the STOE in a secure manner.

AOD_ADM.2.4C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AOD_ADM.2.5C The administrator guidance shall describe all operations regarding user behaviour that are relevant to secure operation of the STOE.

AOD_ADM.2.6C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AOD_ADM.2.7C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the SSF.

AOD_ADM.2.8C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AOD_ADM.2.9C The administrator guidance shall describe all interfaces to external operational systems that are relevant to the administrator.

C.4.4.5.3 Evaluator action elements

AOD_ADM.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOD_ADM.2.2E The evaluator shall independently verify through [selection: *personnel interviews, sampling the administrator guidance*, [assignment: *other methods*]] the practice of the specification of the administrator guidance.

C.4.5 User guidance for an operational system (AOD_USR)

C.4.5.1 Objectives

User guidance for an operational system is intended to be used by non-administrative human users of the STOE. Security policy, procedures, rules, responsibility and other security requirements that are defined by operational requirements and are intended to be used by users should be described in the user guidance. User guidance for an operational system describes the security controls provided by the SSF and provides instructions and guidelines, including warnings, for its secure use.

The user guidance for an operational system provides a basis for operations about the use of the STOE and a measure of confidence that non-malicious users, application providers and others exercising the external interfaces of the STOE will understand the secure operation of the STOE and will use it as intended.

C.4.5.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.4.5.3 Application notes

The content of the user guidance documentation will directly be reflected by the policies, rules, responsibilities, procedures and operational security measures that are related with the user and are defined in the operational controls. The requirement AOD_USR.1.4.C ensures that any warnings to the users of a STOE with regard to the STOE security environment and the security objectives described in the SPP/SST are appropriately covered in the user guidance.

C.4.5.4 AOD_USR.1 User guidance

Dependencies: ASD_SAD.1 Architecture description

C.4.5.4.1 Management action elements

AOD_USR.1.1M The management shall provide user guidance.

C.4.5.4.2 Content and presentation of evidence elements

AOD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the STOE.

AOD_USR.1.2C The user guidance shall describe the operational controls that are related to the user.

AOD_USR.1.3C The user guidance shall describe the use of user-accessible security functions provided by the STOE.

AOD_USR.1.4C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AOD_USR.1.5C The user guidance shall clearly present all user responsibilities necessary for secure operation of the STOE, including those related to user behaviour during system operation.

AOD_USR.1.6C The user guidance shall be consistent with all other documentation supplied for evaluation.

C.4.5.4.3 Evaluator action elements

AOD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.4.5.5 AOD_USR.2 User guidance verification

Hierarchical to: AOD_USR.1 User guidance

Dependencies: ASD_SAD.1 Architecture description

C.4.5.5.1 Management action elements

AOD_USR.2.1M The management shall provide user guidance.

C.4.5.5.2 Content and presentation of evidence elements

AOD_USR.2.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the STOE.

AOD_USR.2.2C The user guidance shall describe the operational controls that are related to the user.

AOD_USR.2.3C The user guidance shall describe the use of user-accessible security functions provided by the STOE.

AOD_USR.2.4C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AOD_USR.2.5C The user guidance shall clearly present all user responsibilities necessary for secure operation of the STOE, including those related to user behaviour during system operation.

AOD_USR.2.6C The user guidance shall be consistent with all other documentation supplied for evaluation.

C.4.5.5.3 Evaluator action elements

AOD_USR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOD_USR.2.2E The evaluator shall independently verify through [selection: *personnel interviews, sampling the user guidance*, [assignment: *other methods*]] the practice of the specification of the user guidance.

C.4.6 Guidance document verification (AOD_GVR)

C.4.6.1 Objectives

The objective is to demonstrate that the guidance documentation is still correct after changes or modifications of system components, system configuration or operational environment.

C.4.6.2 Component levelling

There is one component.

C.4.6.3 AOD_GVR.1 Guidance verification

Dependencies: AOD_OCD.1 Operational system configuration specification

AOD_ADM.1 Administrator guidance

AOD_USR.1 User guidance

C.4.6.3.1 Objectives

In this component, the objective is to demonstrate that the guidance documentation is still correct after changes or modifications to system components, system configuration or operational environment.

C.4.6.3.2 Application notes

This component does not only address changed or modified parts of the operational system guidance documentation, but also other parts that may have become invalid.

C.4.6.3.3 Developer/integrator action elements

AOD_GVR.1.1D After changes or modifications to system components, system configuration or operational environment, the developer/integrator shall perform a verification analysis to check all operational system configuration and guidance documentation remains correct and consistent.

C.4.6.3.4 Content and presentation of evidence elements

AOD_GVR.1.1C For each configuration document, the verification analysis shall show that the document is unaffected by the changes or modifications, or that it has been correctly updated to reflect the changes or modifications.

AOD_GVR.1.2C For each administrator guidance document, the verification analysis shall show that the document is unaffected by the changes or modifications, or that it has been correctly updated to reflect the changes or modifications.

AOD_GVR.1.3C For each user guidance document, the verification analysis shall show that the document is unaffected by the changes or modifications, or that it has been correctly updated to reflect the changes or modifications.

C.4.6.3.5 Evaluator action elements

AOD_GVR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.5 Class ASD: Operational System Architecture, Design and Configuration Documentation

C.5.1 Introduction

The ASD assurance class is closely derived from the ADV class in ISO/IEC 15408-3. However, the development and integration information necessary and appropriate for operational systems is different enough from that defined in the ADV class to require a new class to be defined.

The purpose of this class is to assess the architecture, design and configuration decisions that have been made to insure that they are sufficient and complete in terms of meeting the functional requirements levied against the operational system. It is through the architecture, design and configuration documentation that insight to these decisions is provided. The secondary purpose of this section is to verify that the operational system architecture, design and configuration reflects the security requirements allocated to the various subsystems and components of the operational system. To do this, the security properties of all internal interfaces must be defined, together with those security properties (such as address space separation) that are enforced by one element of the architecture on others.

C.5.2 Architecture description (ASD_SAD)

C.5.2.1 Objectives

The purpose of the operational system architecture description is to present a detailed discussion of the operational system security properties as built in terms of structure (subsystems, components, interfaces to external operational systems), interactions (interfaces, interconnects, data and control flows), and purpose (tractability to security concept of operations and operational system security requirements), and to allocate any varying assurances to parts of the operational system. This information supports understanding and performing various aspects of the operational system evaluation: the allocation of assurances to portions of the operational system, the operational system security concept of operations, the operational system test strategy, plans and procedures. The purpose of the architecture description evidence is to provide a description of the following aspects of the operational system:

a) the definition of subsystems that comprise the operational system;

b) the internal and external interfaces to the subsystems and the functionality provided through the identified interfaces;

c) the interconnects between the subsystems and the information flow between subsystems across the interconnects;

d) the external operational systems to which the operational system interfaces and the relationships between the operational system and these external operational systems;

e) the interconnects to external operational systems and the information flow between the operational system and external operational systems across the interconnects;

f) the measures protecting and enforcing the correct operation of security controls.

C.5.2.2 Component levelling

This family contains one component.

C.5.2.3 ASD_SAD.1 Architecture description

Dependencies: no dependencies.

C.5.2.3.1 Developer/integrator action elements

ASD_SAD.1.1D The developer/integrator shall provide an architecture description.

C.5.2.3.2 Content and presentation of evidence elements

ASD_SAD.1.1C The architecture description shall identify the operational system in terms of its subsystems and the interfaces and interconnects between the subsystems.

ASD_SAD.1.2C The architecture description shall identify the external operational systems that interact with the operational system and the interfaces and interconnects between the operational system and external operational systems.

ASD_SAD.1.3C The architecture description shall describe the purpose and functions of the identified subsystems, interconnects and interfaces of the operational system.

ASD_SAD.1.4C The architecture description shall describe the purpose of the identified interconnects and interfaces from the operational system to external operational systems and shall describe the services from and provided to the external operational systems.

ASD_SAD.1.5C The architecture description shall describe all the operational system security properties that are enforced by one element of the architecture upon others, including measures for the protection of security controls from unauthorized disclosure, modification, destruction and bypassing.

ASD_SAD.1.6C The architecture description shall describe the self-protection mechanisms for security controls.

ASD_SAD.1.7C The architecture description shall be internally consistent.

C.5.2.3.3 Evaluator action elements

ASD_SAD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.5.3 Interface functional specification (ASD_IFS)

C.5.3.1 Objectives

The purpose of the operational system interface functional specification is to provide a description of the operational system security functions accessible at the visible interfaces, and their security properties.

C.5.3.2 Component levelling

This family contains one component.

C.5.3.3 ASD_IFS.1 Interface functional specification

Dependencies: ASD_SAD.1 Architecture description

C.5.3.3.1 Developer/integrator action elements

ASD_IFS.1.1D The developer/integrator shall provide an interface functional specification.

C.5.3.3.2 Content and presentation of evidence elements

ASD_IFS.1.1C The interface functional specification shall identify and describe all the visible operational system interfaces, including the security functions accessible through those interfaces and the security properties of those interfaces.

ASD_IFS.1.2C The interface functional specification shall be internally consistent.

C.5.3.3.3 Evaluator action elements

ASD_IFS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASD_IFS.1.2E The evaluator shall determine that the interface functional specification is consistent with the architecture description.

C.5.4 Subsystem design (ASD_SSD)

C.5.4.1 Objectives

The purpose of the subsystem design evidence is to provide a description of the following:

a) the subsystems;

b) the allocation of security functionality to the subsystems;

c) the security properties of each subsystem;

d) the interfaces to each subsystem and the functionality provided through each interface;

e) the components from which each subsystem is built.

C.5.4.2 Component levelling

This family contains one component.

C.5.4.3 ASD_SSD.1 Subsystem design

Dependencies: ASD_SAD.1 Architecture description

ASD_IFS.1 Interface functional specification

C.5.4.3.1 Developer/integrator action elements

ASD_SSD.1.1D The developer/integrator shall provide a subsystem design.

ASD_SSD.1.2D The developer/integrator shall provide a mapping from the subsystem design to the architecture design.

C.5.4.3.2 Content and presentation of evidence elements

ASD_SSD.1.1C The subsystem design shall describe the security functionality provided by each subsystem.

ASD_SSD.1.2C The subsystem design shall identify all hardware, firmware, and software required by the security functionality allocated to the subsystem.

ASD_SSD.1.3C The subsystem design shall identify the interfaces to each subsystem.

ASD_SSD.1.4C The subsystem design shall identify the security properties for each subsystem.

ASD_SSD.1.5C The subsystem design shall describe the interfaces to each subsystem, in terms of their purpose and method of use of the effects, exceptions and error messages.

ASD_SSD.1.6C The subsystem design shall identify the components from which each subsystem is built.

ASD_SSD.1.7C The subsystem design shall be internally consistent.

ASD_SSD.1.8C The subsystem design shall be a complete instantiation of the operational system security functionality, including domain-specific functionality.

ASD_SSD.1.9C The mapping from subsystem design to architecture design shall demonstrate that all elements of the architecture design are present in the subsystem design.

C.5.4.3.3 Evaluator action elements

ASD_SSD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASD_SSD.1.2E The evaluator shall determine that the subsystem design is consistent with the architecture description and interface functional specification.

C.5.5 Component design (ASD_CMP)

C.5.5.1 Objectives

The purpose of the component design evidence is to provide a description of the following:

a) purpose and functions of each operational system component;

b) the allocation of security functionality to each component;

c) the security properties of each component;

d) the subsystem interfaces provided by each component;

e) the functionality provided through the identified interfaces to the component;

f) how the security functionality and security properties of each component are provided.

C.5.5.2 Component levelling

This family contains one component.

C.5.5.3 ASD_CMP.1 Component design

Dependencies: ASD_IFS.1 Interface functional specification

ASD_SSD.1 Subsystem design

C.5.5.3.1 Developer/integrator action elements

ASD_CMP.1.1D The developer/integrator shall provide a component design.

ASD_CMP.1.2D The developer/integrator shall provide a mapping from the component design to the subsystem design.

ASD_CMP.1.3D The developer/integrator shall provide a STOE summary specification consistency analysis.

C.5.5.3.2 Content and presentation of evidence elements

ASD_CMP.1.1C The component design shall describe the purpose and functions of the components of each subsystem.

ASD_CMP.1.2C The component design shall define the interrelationships between the components in each subsystem.

ASD_CMP.1.3C The component design shall identify the interfaces to the operational system subsystem met by each component.

ASD_CMP.1.4C The component design shall describe the interfaces to the operational system subsystem met by each component in terms of their purpose and method of use.

ASD_CMP.1.5C The component design shall describe the security functionality provided by each component.

ASD_CMP.1.6C The component design shall identify the security properties for each component.

ASD_CMP.1.7C The component design shall describe how the security functionality and security properties of each component are provided.

ASD_CMP.1.8C The component design for each subsystem shall be internally consistent.

ASD_CMP.1.9C The component design for each subsystem shall provide a complete instantiation of the security functionality assigned to that subsystem, including domain-specific functionality.

ASD_CMP.1.10C The mapping from component design to subsystem design shall demonstrate that all elements of the subsystem design are present in the component design.

ASD_CMP.1.11C The STOE summary specification consistency analysis shall demonstrate that the component design is consistent with the description of implementation of SSFs and SSAs in the STOE summary specification and any STOE domain summary specifications.

C.5.5.3.3 Evaluator action elements

ASD_CMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASD_CMP.1.2E The evaluator shall determine that the component design is consistent with the subsystem design and interface functional specification.

C.5.6 Implementation representation (ASD_IMP)

C.5.6.1 Objectives

The purpose of the implementation representation is to support the evaluation of critical operational system functionality developed solely for the purpose of integrating components into the operational system. Critical operational system functionality is not functionality that exists in the component as built or as evaluated. However, it may be necessary for some of the evaluated portions of a component to be revisited in the context of the operational system evaluation as a result of specific configuration or integration issues identified prior to or during the operational system evaluation.

C.5.6.2 Application notes

It is not envisaged that the implementation representation (e.g. source code) is provided for all components of the operational system, only those which configure other portions of the operational system or implement critical security functionality supporting other components. Integration programs or exit routine programs developed solely for the operational system may be target for this family.

C.5.6.3 Component levelling

This family contains one component.

C.5.6.4 ASD_IMP.1 Implementation representation

Dependencies: ASD_CMP.1 Component design

C.5.6.4.1 Developer/integrator action elements

ASD_IMP1.1D The developer/integrator shall provide an implementation representation of the component design.

C.5.6.4.2 Content and presentation of evidence elements

ASD_IMP.1.1C The implementation representation shall be a complete implementation of the component design, including all security functionality and security properties assigned to that component.

ASD_IMP.1.2C The implementation representation shall establish the security functionality provided by each component in terms of its specific configuration requirements.

ASD_IMP.1.3C The implementation representation shall be internally consistent.

C.5.6.4.3 Evaluator action elements

ASD_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.5.7 Security concept of operations (ASD_CON)

C.5.7.1 Objectives

The purpose of the security concept of operations is to describe the security policies, properties and characteristics of the operational system as they are provided and enforced in support of the operational business or mission case. This will permit analysis of the architectural design evidence to confirm that the STOE enforces the necessary policies and properties.

C.5.7.2 Application notes

Different techniques are generally used to ensure the effectiveness of the technical and operational controls implementing the SSF. In the case of technical controls, the necessary pervasive mechanisms are often implemented at the hardware level (e.g. memory management mechanisms). In the case of operational controls, organisation-wide procedural mechanisms are often used (e.g. separation of duties).

C.5.7.3 Component levelling

This family contains one component.

C.5.7.4 ASD_CON.1 Security concept of operations

Dependencies: ASD_SAD.1 Architecture description

C.5.7.4.1 Developer/integrator action elements

ASD_CON.1.1D The system developer/integrator shall provide security concept of operations documentation covering all SSF.

C.5.7.4.2 Content and presentation of evidence elements

ASD_CON.1.1C The security concept of operations documentation shall be at a level of detail commensurate with the description of interfaces, security properties and mechanisms provided in the architectural design.

ASD_CON.1.2C The security concept of operations documentation shall cover all modes of operation of the operational system (e.g. including backup or degraded modes of operation).

ASD_CON.1.3C The security concept of operations documentation shall be internally consistent.

ASD_CON.1.4C The security concept of operations documentation shall describe how the SSF maintains the security domains of the operational system in a manner consistent with the SFRs.

ASD_CON1.5C The security concept of operations documentation shall demonstrate that the SSF initialisation process prevents bypass, interference or tampering with establishment of the SFR-enforcing functionality.

ASD_CON.1.6C The security concept of operations documentation shall demonstrate that the SSF protects itself from interference and tampering.

ASD_CON.1.7C The security concept of operations documentation shall demonstrate that the SSF prevents bypass of SFR-enforcing functionality.

ASD_CON.1.8C The security concept of operations documentation shall demonstrate that information flows between domains of the operational system, and between the operational system and external operational systems, do not bypass, interfere or tamper with the SFR-enforcing functionality.

C.5.7.4.3 Evaluator action elements

ASD_CON.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASD_CON.1.2E The evaluator shall determine whether the architectural design is a complete and correct instantiation of the operational system security concept of operations in support of the operational mission.

C.5.8 Design document verification (ASD_GVR)

C.5.8.1 Objectives

The objective is to demonstrate that the security design documentation is still correct after changes or modifications of system components.

C.5.8.2 Component levelling

There is one component.

C.5.8.3 ASD_GVR.1 Design verification

Dependencies: ASD_SAD.1 Architecture description

ASD_IFS.1 Interface functional specification

ASD_SSD.1 Subsystem design

ASD_CMP.1 Component design

ASD_CON.1 Security concept of operations

C.5.8.3.1 Objectives

In this component, the objective is to demonstrate that the security documentation is still correct after changes or modifications to system components.

C.5.8.3.2 Application notes

This component does not only address changed or modified parts of the operational system design documentation, but also other parts that may have become invalid.

C.5.8.3.3 Developer/integrator action elements

ASD_GVR.1.1D After changes or modifications to system components, system configuration or operational environment, the developer/integrator shall perform a verification analysis to check all operational system design documentation remains correct and consistent.

C.5.8.3.4 Content and presentation of evidence elements

ASD_GVR.1.1C For each design document, the verification analysis shall show that the document is unaffected by the changes or modifications, or that it has been correctly updated to reflect the changes or modifications.

C.5.8.3.5 Evaluator action elements

ASD_GVR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.6 Class AOC: Operational System Configuration Management

C.6.1 Introduction

The objective of Configuration Management during evaluation is to provide assurance that the evaluator has the correct version of all operational system components for the other evaluation activities. It applies therefore to measures within the development and integration environment, not the operational environment where this is different. When the operational system is deployed and integrated, the evaluated configuration management system remains in the development and integration environment.

The configuration management may control evaluated and non-evaluated products in the operational systems.

This class provides the non-IT measures that allow security personnel to manage the security aspects of the operational system and its associated configuration(s) during operations, and to control changes to the operational system related to its security measures. Security configuration management defines and describes the operational system components, as defined by its developmental configuration; its integration configuration, which includes any specialized interoperability functionality; and its operational configuration,

which defines the parameter settings for the runtime configuration of the components. It also provides for change control policies and procedures are in place and effectively implemented to control changes to the operational system, including access restrictions for change control.

The families in this class define the processes and procedures that will allow security personnel to determine what comprises the operational system configuration. It permits the tracking and maintenance of the operational system and each of the critical components that comprise the operational system in the various configurations. The configuration definitions include developmental, integration, operational, and contingency. The families would necessarily define the non-IT measures that contribute to operational system security, and provide requisite configuration control and an audit trail related to changes in operational system security activity.

C.6.2 Operational system baseline configuration (AOC_OBM)

C.6.2.1 Objectives

This family defines the evaluated operational system configuration and its security components, and the means by which security configuration management plans and procedures track the baseline configuration and control changes to that baseline. It essentially tracks, manages and controls the evaluated operational system baseline, and the means by which security configuration management tracks and controls change to that baseline. This family identifies and tracks both the technical and operational controls that contribute to the operational system security function, and their inter-relationships. The operational system baseline will be updated upon each re-evaluation to reflect the latest evaluated baseline to which any subsequent modifications, impact analysis or re-evaluations will reference.

C.6.2.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.6.2.3 AOC_OBM.1 Operational system baseline configuration

Dependencies: no dependencies.

C.6.2.3.1 Developer/integrator action elements

AOC_OBM.1.1D The developer/integrator shall use a CM system for the initial/most recent evaluated system, which shall be called the "Baseline".

AOC_OBM.1.2D The CM system shall track and monitor each change, proposed and actual to the system Baseline, and its evaluation status.

AOC_OBM.1.3D The CM system shall report the current operational system configuration baseline.

AOC_OBM.1.4D The developer/integrator/system owner shall provide CM documentation of the Baseline system.

C.6.2.3.2 Content and presentation of evidence elements

AOC_OBM.1.1C The CM system shall uniquely identify the STOE Baseline, each associated change, and its evaluation status.

AOC_OBM.1.2C The CM plan shall describe how the system baseline is maintained, and changes to the baseline are tracked and controlled.

C.6.2.3.3 Evaluator action elements

AOC_OBM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.6.2.4 AOC_OBM.2 Operational system baseline configuration verification

Hierarchical to: AOC_OBM.1 Operational system baseline configuration

Dependencies: no dependencies.

C.6.2.4.1 Developer/integrator action elements

AOC_OBM.2.1D The developer/integrator shall use a CM system for the initial/most recent evaluated system, which shall be called the “Baseline”.

AOC_OBM.2.2D The CM system shall track and monitor each change, proposed and actual to the system Baseline, and its evaluation status.

AOC_OBM.2.3D The CM system shall report the current operational system configuration baseline.

AOC_OBM.2.4D The developer/integrator/system owner shall provide CM documentation of the Baseline system.

C.6.2.4.2 Content and presentation of evidence elements

AOC_OBM.2.1C The CM system shall uniquely identify the STOE Baseline, each associated change, and its evaluation status.

AOC_OBM.2.2C The CM plan shall describe how the system baseline is maintained, and changes to the baseline are tracked and controlled.

C.6.2.4.3 Evaluator action elements

AOC_OBM.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOC_OBM.2.2E The evaluator shall independently verify through [selection: *personnel interviews, sampling the changes*, [assignment: *other methods*]] the veracity of the CM system.

C.6.3 Evaluated component products (AOC_ECP)

C.6.3.1 Objectives

This family defines the assurance package and operational parameter requirements for operational system components that are made up from evaluated products. When creating an operational system from product components, there is a need to specify the required assurance from aspects of development and integration activities. Where COTS products are used, there will normally be no development activities performed specifically for the operational system. Assurance must therefore be obtained from product evaluation and certification, such as availability of a formal certificate stating that a product has been certified, for example, at EAL4, as defined in ISO/IEC 15408.

C.6.3.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.6.3.3 AOC_ECP.1 Evaluated component products

Dependencies: AOC_OBM.1 Operational system baseline configuration

C.6.3.3.1 Developer/integrator action elements

AOC_ECP.1.1D The developer/integrator shall define evaluated assurance packages for component products or security domains containing such products.

AOC_ECP.1.2D The developer/integrator shall specify operational parameters for each component product.

C.6.3.3.2 Content and presentation of evidence elements

AOC_ECP.1.1C The CM plan shall describe the evaluated assurance packages for component products or security domains containing such products.

AOC_ECP.1.2C The statement of evaluation results or independent certification report and the ST for evaluated products shall be identified.

AOC_ECP.1.3C The CM plan shall describe the operational parameters for each component product.

C.6.3.3.3 Evaluator action elements

AOC_ECP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.6.3.4 AOC_ECP.2 Evaluated component products verification

Hierarchical to: AOC_ECP.1 Evaluated component products

Dependencies: AOC_OBM.1 Operational system baseline configuration

C.6.3.4.1 Developer/integrator action elements

AOC_ECP.2.1D The developer/integrator shall define evaluated assurance packages for component products or security domains containing such products.

AOC_ECP.2.2D The developer/integrator shall specify operational parameters for each component product.

C.6.3.4.2 Content and presentation of evidence elements

AOC_ECP.2.1C The CM plan shall describe the evaluated assurance packages for component products or security domains containing such products.

AOC_ECP.2.2C The statement of evaluation results or independent certification report and the ST for evaluated products shall be identified.

AOC_ECP.2.3C The CM plan shall describe the operational parameters for each component product.

C.6.3.4.3 Evaluator action elements

AOC_ECP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOC_ECP.2.2E The evaluator shall confirm that the operational conditions described in the statement of evaluation results or independent certification report of the evaluated products meet the requirements of the operational environment of the operational system.

C.6.4 Conformance with PPs (AOC_PPC)

C.6.4.1 Objectives

This family defines the assurance requirements for conformance with a specific PP. The evidence to be provided will be a certification report including the applicable ST. In the operational environment, product components may have specific parameters for operation. Such parameters must be defined correctly.

C.6.4.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.6.4.3 AOC_PPC.1 Conformance with PPs

Dependencies: AOC_OBM.1 Operational system baseline configuration

C.6.4.3.1 Developer/integrator action elements

AOC_PPC.1.1D The developer/integrator shall specify PPs for component products to be in compliance with.

AOC_PPC.1.2D The developer/integrator shall specify operational parameters for each component product.

C.6.4.3.2 Content and presentation of evidence elements

AOC_PPC.1.1C The CM plan shall specify PPs for component products to be in compliance with.

AOC_PPC.1.2C The statement of evaluation results or independent certification report and the ST for evaluated products shall be identified.

AOC_PPC.1.3C The CM plan shall describe the operational parameters for each component product.

C.6.4.3.3 Evaluator action elements

AOC_PPC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.6.4.4 AOC_PPC.2 Conformance with PPs verification

Hierarchical to: AOC_PPC.1 Conformance with PPs

Dependencies: AOC_OBM.1 Operational system baseline configuration

C.6.4.4.1 Developer/integrator action elements

AOC_PPC.2.1D The developer/integrator shall specify PPs for component products to be in compliance with.

AOC_PPC.2.2D The developer/integrator shall specify operational parameters for each component product.

C.6.4.4.2 Content and presentation of evidence elements

AOC_PPC.2.1C The CM plan shall specify PPs for component products to be in compliance with.

AOC_PPC.2.2C The statement of evaluation results or independent certification report and the ST for evaluated products shall be identified.

AOC_PPC.2.3C The CM plan shall describe the operational parameters for each component product.

C.6.4.4.3 Evaluator action elements

AOC_PPC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOC_PPC.2.2E The evaluator shall confirm that the operational conditions described in the statement of evaluation results or independent certification report of the evaluated products meet the requirements of the operational environment of the operational system.

C.6.5 Non-evaluated component products (AOC_NCP)

C.6.5.1 Objectives

This family defines the assurance package and operational parameter requirements for operational system components that are made up from non-evaluated products. When creating an operational system from product components, there is a need to specify the required assurance from aspects of development and integration activities. For products such as business application programs that are developed for the operational system specifically, during their development activities the same assurance evidence as required for product evaluation can be produced by the product developer.

In the operational environment, product components may have specific parameters for operation. Such parameters must be defined correctly.

C.6.5.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.6.5.3 AOC_NCP.1 Non-evaluated component products

Dependencies: AOC_OBM.1 Operational system baseline configuration

C.6.5.3.1 Developer/integrator action elements

AOC_NCP.1.1D The developer/integrator/system owner shall define required assurance packages for component products or security domains containing such products.

AOC_NCP.1.2D The developer/integrator/system operator shall specify operational parameters for each component product.

C.6.5.3.2 Content and presentation of evidence elements

AOC_NCP.1.1C The CM plan shall describe the required assurance packages for component products or security domains containing such products.

AOC_NCP.1.2C The CM plan shall describe the operational parameters for each component product.

C.6.5.3.3 Evaluator action elements

AOC_NCP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.6.5.4 AOC_NCP.2 Non-evaluated component products verification

Hierarchical to: AOC_NCP.1 Non-evaluated component products

Dependencies: AOC_OBM.1 Operational system baseline configuration

C.6.5.4.1 Developer/integrator action elements

AOC_NCP.2.1D The developer/integrator/system owner shall define required assurance packages for component products or security domains containing such products.

AOC_NCP.2.2D The developer/integrator/system operator shall specify operational parameters for each component product.

C.6.5.4.2 Content and presentation of evidence elements

AOC_NCP.2.1C The CM plan shall describe the required assurance packages for component products or security domains containing such products.

AOC_NCP.2.2C The CM plan shall describe the operational parameters for each component product.

C.6.5.4.3 Evaluator action elements

AOC_NCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOC_NCP.2.2E The evaluator shall conduct the evaluation and confirm that the products meet the required assurance packages under the operational environment of the operational system.

C.7 Class AOT: Operational System Test

C.7.1 Introduction

The purpose of this class is to verify that the operational system components, when installed, integrated and configured in accordance with the operational system architecture and operational system configuration evidence, meet the security functional requirements specified in the SST and are effective in enforcing the operational system security concept of operations. Operational system architecture, integration and design documentation aid in test plan and execution. This is accomplished by determining that the SSF has been configured as specified by the configuration specification, tested against the relevant architecture and design evidence, by performing a sample of the developer/integrator's tests, and by independently testing a subset of the SSF.

C.7.2 Operational system functional tests (AOT_FUN)

C.7.2.1 Objectives

The objective of this component is for the developer to demonstrate that all security functions perform as specified. The developer is required to perform testing and to provide test documentation.

Functional testing performed by the developer and/or integrator establishes that the SSF exhibits the properties necessary to satisfy the functional requirements of its PP/ST. Such functional testing provides assurance that the SSF satisfies at least the security functional requirements, although it cannot establish that the SSF does no more than what was specified. The family "Functional tests" is focused on the type and amount of documentation or support tools required, and what is to be demonstrated through developer testing. Functional testing is not limited to positive confirmation that the required security functions are provided, but may also include negative testing to check for the absence of particular undesired behaviour (often based on the inversion of functional requirements).

This family contributes to providing assurance that the likelihood of undiscovered flaws is relatively small.

The families AOT_COV, AOT_DPT and AOT_FUN are used in combination to define the evidence of testing to be supplied by a developer and/or an integrator. Independent functional testing by the evaluator is specified by AOT_IND.

C.7.2.2 Component levelling

This family contains one component.

C.7.2.3 Application notes

Procedures for performing tests are expected to provide instructions for using test programs and test suites, including the test environment, test conditions, test data parameters and values. The test procedures should also show how the test results are derived from the test inputs.

This family specifies requirements for the presentation of all test plans, procedures and results. Thus the quantity of information that must be presented will vary in accordance with the use of AOT_COV and AOT_DPT.

Ordering dependencies are relevant when the successful execution of a particular test depends upon the existence of a particular state. For example, this might require that test A be executed immediately before test B, since the state resulting from the successful execution of test A is a prerequisite for the successful execution of test B. Thus, failure of test B could be related to a problem with the ordering dependencies. In the above example, test B could fail because test C (rather than test A) was executed immediately before it, or the failure of test B could be related to a failure of test A.

C.7.2.4 AOT_FUN.1 Functional testing

Dependencies: no dependencies.

C.7.2.4.1 Developer/integrator action elements

AOT_FUN.1.1D The developer/integrator shall test the SSF and document the results.

AOT_FUN.1.2D The developer/integrator shall provide test documentation.

AOT_FUN.1.3D The developer/integrator shall provide an analysis of level of detail of integrated security controls testing.

C.7.2.4.2 Content and presentation of evidence elements

AOT_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

AOT_FUN.1.2C The analysis of the security controls verification shall demonstrate that the correspondence between the security controls as identified in the SST and the tests identified in the test documentation is complete.

AOT_FUN.1.3C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

AOT_FUN.1.4C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

AOT_FUN.1.5C The expected test results shall show the anticipated outputs from a successful execution of the tests.

AOT_FUN.1.6C The test results from the developer/integrator execution of the tests shall demonstrate that each tested security function behaved as specified.

AOT_FUN.1.7C The test documentation shall include an analysis of the test procedure ordering dependencies.

C.7.2.4.3 Evaluator action elements

AOT_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.7.3 Operational system test coverage (AOT_COV)

C.7.3.1 Objectives

This family addresses those aspects of testing that deal with completeness of test coverage. That is, it addresses the extent to which the SSF is tested, and whether or not the testing is sufficiently extensive to demonstrate that the SSF operates as specified.

C.7.3.2 Component levelling

This family has two components. The components in this family are levelled on the basis of increasing rigor of interface testing, and increasing rigor of the analysis of the sufficiency of the tests to demonstrate that the SSF operates in accordance with its interface functional specification.

C.7.3.3 AOT_COV.1 Evidence of coverage

Dependencies: ASD_IFS.1 Interface functional specification

AOT_FUN.1 Functional testing

C.7.3.3.1 Objectives

The objective of this component is to establish that the SSF has been tested against the interface functional specification in a systematic manner. This is to be achieved through an examination of developer and/or integrator analysis of correspondence.

C.7.3.3.2 Application notes

While the testing objective is to cover the SSF, there is no requirement to provide anything to verify this assertion other than an informal mapping of tests to the interface functional specification and the testing data itself.

In this component the developer/integrator is required to demonstrate that the tests which have been identified include testing of all of the visible security functions as described in the interface functional specification. The analysis should not only show the correspondence between tests and security functions, but should provide also sufficient information for the evaluator to determine how the functions have been exercised. This information can be used in planning for additional evaluator tests. Although at this level the developer/integrator has to demonstrate that each of the functions within the interface functional specification has been tested, the amount of testing of each function need not be exhaustive.

C.7.3.3.3 Developer/integrator action elements

AOT_COV.1.1D The developer/integrator shall provide an analysis of the test coverage.

C.7.3.3.4 Content and presentation of evidence elements

AOT_COV.1.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the SSF accessible through visible operational system interfaces as described in the interface functional specification.

AOT_COV.1.2C The analysis of the test coverage shall demonstrate that the correspondence between the SSF accessible through visible operational system interfaces as described in the interface functional specification and the tests identified in the test documentation is complete.

C.7.3.3.5 Evaluator action elements

AOT_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.7.3.4 AOT_COV.2 Rigorous analysis of coverage

Hierarchical to: AOT_COV.1 Evidence of coverage

Dependencies: ASD_IFS.1 Interface functional specification

AOT_FUN.1 Functional testing

C.7.3.4.1 Objectives

The objective of this component is to establish that the SSF has been tested against its interface functional specification in a systematic and exhaustive manner. This is to be achieved through an examination of developer analysis of correspondence.

C.7.3.4.2 Application notes

The developer/integrator is required to provide a convincing argument that the tests which have been identified cover all visible security functions, and that the testing of each security function is complete. There will remain little scope for the evaluator to devise additional functional tests of the SSF interfaces based on the interface functional specification, as they will have been exhaustively tested. Nevertheless, the evaluator should strive to devise such tests.

C.7.3.4.3 Developer/integrator action elements

AOT_COV.2.1D The developer/integrator shall provide an analysis of the test coverage.

C.7.3.4.4 Content and presentation of evidence elements

AOT_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the SSF accessible through visible operational system interfaces as described in the interface functional specification.

AOT_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the SSF accessible through visible operational system interfaces as described in the interface functional specification and the tests identified in the test documentation is complete.

AOT_COV.2.3C The analysis of the test coverage shall rigorously demonstrate that all visible interfaces to the SSF identified in the interface functional specification have been completely tested.

C.7.3.4.5 Evaluator action elements

AOT_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.7.4 Operational system depth of testing (AOT_DPT)

C.7.4.1 Objectives

The components in this family deal with the level of detail to which the SSF is tested. Testing of security functions is based upon increasing depth of information derived from analysis of the representations.

The objective is to counter the risk of missing an error in the development and integration of the STOE. Additionally, the components of this family, especially as testing is more concerned with the internal structure of the SSF, are more likely to discover any malicious code that has been inserted.

Testing that exercises specific internal interfaces can provide assurance not only that the SSF exhibits the desired external security behaviour, but also that this behaviour stems from correctly operating internal mechanisms.

C.7.4.2 Component levelling

This family has three components. The components in this family are levelled on the basis of increasing detail provided in the SSF representations, from the architecture design to the implementation representation. This levelling reflects the SSF representations presented in the ASD class.

C.7.4.3 Application notes

The specific amount and type of documentation and evidence will, in general, be determined by the chosen component from AOT_FUN.

Testing at the level of the interface functional specification is addressed by AOT_COV.

The principle adopted within this family is that the level of testing be appropriate to the level of assurance being sought. Where higher components are applied, the test results will need to demonstrate that the implementation of the SSF is consistent with its design. For example, the subsystem design should describe each of the subsystems and also describe the interfaces between these subsystems in sufficient detail for the purpose, effects and errors of each interface to be clearly defined. Evidence of testing at the subsystem design level must show that the internal interfaces between subsystems have been exercised. This may be achieved through testing via the external interfaces of the SSF, or by testing of the subsystem interfaces in isolation, perhaps employing a test harness. The higher components in this family aim to check the correct operation of internal interfaces that become visible as the design becomes less abstract. When these components are applied it will be more difficult to provide adequate evidence of the depth of testing using the SSF's external interfaces alone.

C.7.4.4 AOT_DPT.1 Testing: interface functional specification

Dependencies: ASD_IFS.1 Interface functional specification

AOT_FUN.1 Functional testing

C.7.4.4.1 Objectives

The interface functional specification identifies and describes all the SSF accessible through externally visible interfaces. Testing at the level of the visible interfaces provides assurance that the directly accessible SSF have been correctly realized.

C.7.4.4.2 Developer/integrator action elements

AOT_DPT.1.1D The developer/integrator shall provide an analysis of the depth of testing.

C.7.4.4.3 Content and presentation of evidence elements

AOT_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the SSF operates in accordance with its interface functional specification.

C.7.4.4.4 Evaluator action elements

AOT_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.7.4.5 AOT_DPT.2 Testing: subsystem design

Hierarchical to: AOT_DPT.1 Testing: interface functional specification

Dependencies: ASD_IFS.1 Interface functional specification

ASD_SSD.1 Subsystem design

AOT_FUN.1 Functional testing

C.7.4.5.1 Objectives

The subsystem design provides a high-level description of the internal workings of the SSF. Testing at the level of the subsystems provides assurance that the SSF subsystems have been correctly realized.

C.7.4.5.2 Developer/integrator action elements

AOT_DPT.2.1D The developer/integrator shall provide an analysis of the depth of testing.

C.7.4.5.3 Content and presentation of evidence elements

AOT_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the SSF operates in accordance with its interface functional specification **and subsystem design**.

C.7.4.5.4 Evaluator action elements

AOT_DPT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.7.4.6 AOT_DPT.3 Testing: component design

Hierarchical to: AOT_DPT.2 Testing: subsystem design

Dependencies: ASD_IFS.1 Interface functional specification

ASD_SSD.1 Subsystem design

ASD_CMP.1 Component design

AOT_FUN.1 Functional testing

C.7.4.6.1 Objectives

The component design provides a detailed description of the internal workings of the SSF. Testing at the level of the components provides assurance that the detailed design of all SSFs have been correctly realized.

C.7.4.6.2 Developer/integrator action elements

AOT_DPT.3.1D The developer/integrator shall provide an analysis of the depth of testing.

C.7.4.6.3 Content and presentation of evidence elements

AOT_DPT.3.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the SSF operates in accordance with its interface functional specification, subsystem design **and component design**.

C.7.4.6.4 Evaluator action elements

AOT_DPT.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.7.4.7 AOT_DPT.4 Testing: implementation representation

Hierarchical to: AOT_DPT.3 Testing: component design

Dependencies: ASD_IFS.1 Interface functional specification

ASD_SSD.1 Subsystem design

ASD_CMP.1 Component design

ASD_IMP.1 Implementation representation

AOT_FUN.1 Functional testing

C.7.4.7.1 Objectives

The implementation representation of a SSF determines its actual behaviour. Testing at the level of the implementation representation provides assurance that the relevant SSFs have been correctly implemented in all ways.

C.7.4.7.2 Application notes

The implementation representation is the one which is used to generate the SSF itself (e.g. source code which is then compiled).

C.7.4.7.3 Developer/integrator action elements

AOT_DPT.4.1D The developer/integrator shall provide an analysis of the depth of testing.

C.7.4.7.4 Content and presentation of evidence elements

AOT_DPT.4.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the SSF operates in accordance with its architecture design, subsystem design, component design **and implementation representation**.

C.7.4.7.5 Evaluator action elements

AOT_DPT.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.7.5 Independent testing (AOT_IND)

C.7.5.1 Objectives

One objective is to demonstrate that the security functions perform as specified.

An additional objective is to counter the risk of an incorrect assessment of the test outcomes on the part of the developer that results in the incorrect implementation of the specifications, or overlooks code that is non-compliant with the specifications.

C.7.5.2 Component levelling

This family has three components. Levelling is based upon the amount of test documentation, test support and the amount of evaluator testing.

C.7.5.3 Application notes

The testing specified in this family can be supported by a party with specialized knowledge other than the evaluator (e.g. an independent laboratory, an objective consumer organization). Testing requires an understanding of the STOE consistent with the performance of other assurance activities, and the evaluator retains responsibility for ensuring that the requirements of this family are properly addressed when such support is used.

This family deals with the degree to which there is independent functional testing of the SSF. Independent functional testing may take the form of repeating the developer's functional tests, in whole or in part. It may also take the form of the augmentation of the developer's functional tests, either to extend the scope or the depth of the developer's tests, or to test for obvious public security domain security weaknesses that could be applicable to the STOE. These activities are complementary, and an appropriate mix must be planned for each STOE, which takes into account the availability and coverage of test results, and the functional complexity of the SSF. A test plan should be developed that is consistent with the level of other assurance activities, and which, as greater assurance is required, includes larger samples of repeated tests, and more independent positive and negative functional tests by the evaluator.

Sampling of developer tests is intended to provide confirmation that the developer has carried out his planned test program on the SSF, and has correctly recorded the results. The size of sample selected will be influenced by the detail and quality of the developer's functional test results. The evaluator will also need to consider the scope for devising additional tests, and the relative benefit that may be gained from effort in these two areas. It is recognized that repetition of all developer tests may be feasible and desirable in some cases, but may be very arduous and less productive in others. The highest component in this family should therefore be used with caution. Sampling will address the whole range of test results available, including those supplied to meet the requirements of both AOT_COV and AOT_DPT.

There is also a need to consider the different configurations of the STOE that are included within the evaluation. The evaluator will need to assess the applicability of the results provided, and to plan his own testing accordingly.

Independent functional testing is distinct from penetration testing, the latter being based on an informed and systematic search for vulnerabilities in the design and/or implementation. Penetration testing is specified using the family AOV_VLA.

The suitability of the STOE for testing is based on the access to the STOE, and the supporting documentation and information required (including any test software or tools) to run tests. The need for such support is addressed by the dependencies to other assurance families.

Additionally, suitability of the STOE for testing may be based on other considerations. For example, the version of the STOE submitted by the developer may not be the final version.

References to a subset of the SSF are intended to allow the evaluator to design an appropriate set of tests which is consistent with the objectives of the evaluation being conducted.

C.7.5.4 AOT_IND.1 Independent testing - conformance

Dependencies: ASD_IFS.1 Interface functional specification

AOD_ADM.1 Administrator guidance

AOD_USR.1 User guidance

C.7.5.4.1 Objectives

In this component, the objective is to demonstrate that the security functions perform as specified.

C.7.5.4.2 Application notes

This component does not address the use of developer test results. It is applicable where such results are not available, and also in cases where the developer's testing is accepted without validation. The evaluator is required to devise and conduct tests with the objective of confirming that the STOE security functional requirements are met. The approach is to gain confidence in correct operation through representative testing, rather than to conduct every possible test. The extent of testing to be planned for this purpose is a methodology issue, and needs to be considered in the context of a particular STOE and the balance of other evaluation activities.

C.7.5.4.3 Developer/integrator action elements

AOT_IND.1.1D The developer/integrator shall provide the STOE for testing.

C.7.5.4.4 Content and presentation of evidence elements

AOT_IND.1.1C The STOE shall be suitable for testing.

C.7.5.4.5 Evaluator action elements

AOT_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOT_IND.1.2E The evaluator shall test a subset of the SSF as appropriate to confirm that the STOE operates as specified.

C.7.5.5 AOT_IND.2 Independent testing - sample

Hierarchical to: AOT_IND.1 Independent testing - conformance

Dependencies: ASD_IFS.1 Interface functional specification

AOD_ADM.1 Administrator guidance

AOD_USR.1 User guidance

AOT_FUN.1 Functional testing

C.7.5.5.1 Objectives

The objective is to demonstrate that the security functions perform as specified.

Evaluator testing includes selecting and repeating a sample of the developer tests.

C.7.5.5.2 Application notes

The intent is that the developer should provide the evaluator with materials necessary for the efficient reproduction of developer tests. This may include such things as machine-readable test documentation, test programs, etc.

This component contains a requirement that the evaluator has available test results from the developer to supplement the program of testing. The evaluator will repeat a sample of the developer's tests to gain confidence in the results obtained.

Having established such confidence the evaluator will build upon the developer's testing by conducting additional tests that exercise the STOE in a different manner.

By using a platform of validated developer test results the evaluator is able to gain confidence that the STOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. Having gained confidence that the developer has tested the STOE, the evaluator will also have more freedom, where appropriate, to concentrate testing in areas where examination of documentation or specialist knowledge has raised particular concerns.

C.7.5.5.3 Developer/integrator action elements

AOT_IND.2.1D The developer/integrator shall provide the STOE for testing.

C.7.5.5.4 Content and presentation of evidence elements

AOT_IND.2.1C The STOE shall be suitable for testing.

AOT_IND.2.2C The developer/integrator shall provide an equivalent set of resources to those that were used in the developer's functional testing of the SSF.

C.7.5.5.5 Evaluator action elements

AOT_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOT_IND.2.2E The evaluator shall test a subset of the SSF as appropriate to confirm that the STOE operates as specified.

AOT_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

C.7.5.6 AOT_IND.3 Independent testing - complete

Hierarchical to: AOT_IND.2 Independent testing - sample

Dependencies: ASD_IFS.1 Interface functional specification

AOD_ADM.1 Administrator guidance

AOD_USR.1 User guidance

AOT_FUN.1 Functional testing

C.7.5.6.1 Objectives

The objective is to demonstrate that all security functions perform as specified.

Evaluator testing includes repeating all of the developer tests.

C.7.5.6.2 Application notes

The intent is that the developer should provide the evaluator with materials necessary for the efficient reproduction of developer/integrator tests. This may include such things as machine-readable test documentation, test programs, etc.

In this component the evaluator must repeat all of the developer's tests as part of the program of testing. As in the previous component the evaluator will also conduct tests that aim to exercise the STOE in a different manner from that achieved by the developer. In cases where developer testing has been exhaustive, there may remain little scope for this.

C.7.5.6.3 Developer/integrator action elements

AOT_IND.3.1D The developer/integrator shall provide the STOE for testing.

C.7.5.6.4 Content and presentation of evidence elements

AOT_IND.3.1C The STOE shall be suitable for testing.

AOT_IND.3.2C The developer/integrator shall provide an equivalent set of resources to those that were used in the developer's functional testing of the SSF.

C.7.5.6.5 Evaluator action elements

AOT_IND.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOT_IND.3.2E The evaluator shall test a subset of the SSF as appropriate to confirm that the STOE operates as specified.

AOT_IND.3.3E The evaluator shall execute **all** tests in the test documentation to verify the developer test results.

C.7.6 Regression testing (AOT_REG)

C.7.6.1 Objectives

The objective is to demonstrate that the security functions perform as specified after changes or modifications of system components, system configuration or operational environment.

C.7.6.2 Component levelling

There is one component.

C.7.6.3 AOT_REG.1 Regression testing

Dependencies: no dependencies.

C.7.6.3.1 Objectives

In this component, the objective is to demonstrate that the security functions perform as specified after changes or modifications of system components, system configuration or operational environment.

C.7.6.3.2 Application notes

This component does not only address the test of changes or modified parts of the operational system, but also other parts.

C.7.6.3.3 Developer/integrator action elements

AOT_REG.1.1D The developer/integrator shall test a sample of developer tests for SSFs and document the results.

AOT_REG.1.2D The developer/integrator shall provide test documentation.

AOT_REG.1.3D The developer/integrator shall provide an analysis of level of detail of regression testing.

C.7.6.3.4 Content and presentation of evidence elements

AOT_REG.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

AOT_REG.1.2C The test plans shall identify the effects caused by changes or modifications and security functions to be tested and describe the goal of the tests to be performed.

AOT_REG.1.3C The test procedure descriptions shall identify the tests to be performed for changed or modified parts and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the changed parts and results of other tests.

AOT_REG.1.4C The test results from the developer/integrator execution of the tests shall demonstrate that each tested security function behaved as specified and the changes or modifications do not affect the SSFs.

AOT_REG.1.5C The test documentation shall include an analysis of the test procedure ordering dependencies.

C.7.6.3.5 Evaluator action elements

AOT_REG.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.8 Class AOV: Operational System Vulnerability Analysis

C.8.1 Introduction

The purpose of the vulnerability assessment activity is to determine the existence and exploitability of flaws or weaknesses in the operational system as configured for, and implemented in its intended environment. This determination is based upon analysis performed by the developer/integrator and the evaluator, with inputs from the consumer; and is supported by evaluator testing.

Inherently, the vulnerability analysis activity is closely related to the operational system security policy and procedures, physical security measures, personnel security, and having security infrastructure in place to effectively counter any operational system vulnerabilities. The operational system strength of security function encompasses security control aspects (specifically human) to ensure that the operational system remains secure and any breaches can be effectively countered.

C.8.2 Operational System Misuse (AOV_MSU)

C.8.2.1 Objectives

The objectives are to minimize the probability of configuring or installing the STOE, IT and non-IT components, in a way that is non-secure, without the user, or maintainer being able to detect it; and to minimize the risk of human or other errors in operation that may deactivate, disable, or fail to activate security functions, resulting in an undetected non-secure state.

C.8.2.2 Application notes

Conflicting, misleading, incomplete, non-user friendly, or unreasonable guidance may result is a user of the STOE, or any of its subsystems, or components, believing that the STOE is secure, when it is not, and can result in vulnerabilities.

An example of conflicting guidance would be two guidance instructions that imply different outcomes when the same input is applied.

An example of misleading guidance would the description of a single guidance instruction that could be parsed in more than one way, one of which may result in a non-secure state.

An example of incomplete guidance would be a list of significant physical security requirements that omitted a critical item that resulted in that item being overlooked by an administrator, user or maintainer who believe the list of required items to be complete.

An example of non-user friendly guidance would be guidance instructions that were not clearly written, written with too much detail so as to be needlessly complex, and not easily understood by an administrator, user or maintainer, such that the action would be done incorrectly, or perhaps not done at all; and may result in an incorrect or unnecessary action which would result in the operational system being put in a non-secure state.

An example of unreasonable guidance would be a recommendation to follow a procedure that imposed an unduly onerous administrative, user, or maintenance burden.

Guidance documentation is required. The requisite documentation may be contained in existing documentation for the STOE, or provided separately. If provided separately, the evaluator should confirm that the documentation is supplied with the STOE.

C.8.2.3 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.8.2.4 AOV_MSU.1 Examination of operational system guidance

Dependencies: AOD_ADM.1 Administrator guidance

AOD_USR.1 User guidance

C.8.2.4.1 Objectives

The objective is to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

C.8.2.4.2 Developer/integrator action elements

AOV_MSU.1.1D The developer/integrator shall provide guidance documentation.

AOV_MSU.1.2D The developer/integrator shall document an analysis of the guidance documentation.

C.8.2.4.3 Content and presentation of evidence elements

AOV_MSU.1.1C The guidance documentation shall identify all possible modes of operation of the STOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AOV_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AOV_MSU.1.3C The guidance documentation shall describe all operational controls.

AOV_MSU.1.4C The guidance documentation shall describe all dependencies on secure operation of external operational systems.

AOV_MSU.1.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

C.8.2.4.4 Evaluator action elements

AOV_MSU.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOV_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the STOE can be configured and used securely using only the supplied guidance documentation.

AOV_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected and to be recovered to secure state.

AOV_MSU.1.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the STOE.

C.8.2.5 AOV_MSU.2 Analysis and testing for insecure states

Hierarchical to: AOV_MSU.1 Examination of operational system guidance

Dependencies: AOD_ADM.1 Administrator guidance

AOD_USR.1 User guidance

C.8.2.5.1 Objectives

The objective is to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. In this component, an analysis of the guidance documentation by the developer is required to provide additional assurance that the objective has been met, and this analysis is validated and confirmed through testing by the evaluator.

C.8.2.5.2 Application notes

In this component the evaluator is required to undertake testing to ensure that if and when the STOE enters an insecure state this may easily be detected. This testing may be considered as a specific aspect of penetration testing.

C.8.2.5.3 Developer/integrator action elements

AOV_MSU.2.1D The developer/integrator shall provide guidance documentation**.**

AOV_MSU.2.2D The developer/integrator shall document an analysis of the guidance documentation.

C.8.2.5.4 Content and presentation of evidence elements

AOV_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the STOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AOV_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AOV_MSU.2.3C The guidance documentation shall describe all operational controls.

AOV_MSU.2.4C The guidance documentation shall describe all dependencies on secure operation of external operational systems.

AOV_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

C.8.2.5.5 Evaluator action elements

AOV_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOV_MSU.2.2E The evaluator shall repeat all configuration and installation procedures to confirm that the STOE can be configured and used securely using only the supplied guidance documentation.

AOV_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected and to be recovered to secure state.

AOV_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the STOE.

AOV_MSU.2.5E The evaluator shall perform independent testing to determine that an administrator or user, with an understanding of the guidance documentation, would reasonably be able to determine if the STOE is configured and operating in a manner that is insecure.

C.8.3 Vulnerability analysis (AOV_VLA)

C.8.3.1 Objective

Vulnerability analysis is an assessment to determine whether vulnerabilities identified during the evaluation of the construction and anticipated operation of the STOE, or by other methods (e.g., by flaw hypothesis), throughout the operational system's life cycle, allow the ability to interfere with or alter the SSF, or interfere with the authorized capabilities of other users.

C.8.3.2 Application notes

A vulnerability analysis is performed by the developer/integrator, in order to identify the presence of security vulnerabilities, and should consider the contents of all of the STOE deliverables. The disposition of identified vulnerabilities will be documented to allow the evaluator to utilize that information, as required, to support the evaluator's independent penetration testing and/or vulnerability analysis.

The intent of the vulnerability analysis is to confirm that no identified security vulnerabilities can be exploited in the intended environment of the STOE and that the STOE is resistant to obvious penetration attacks.

Obvious vulnerabilities are considered to be those that are open to exploitation that require a minimum of understanding of the STOE, both its non-IT and IT components, and a minimum of skill, technical sophistication, and resources. These might be suggested by the SSF interface description. Obvious vulnerabilities include those in the public security domain, details of which should be known to the developer/integrator, and the user organization, or available from an evaluation authority.

Performing a search for vulnerabilities in a systematic way requires that the developer/integrator works in a structured and repeatable way, as opposed to identifying vulnerabilities in an ad hoc fashion.

Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer/integrator to search for further vulnerabilities.

The main intent of the independent evaluator vulnerability analysis and associated penetration testing is to determine that the STOE is resistant to penetration attacks performed by an attacker possessing a low (for AOV_VLA.2), to moderate (for AOV_VLA.3) or high (for AOV_VLA.4) attack potential. The evaluator should assume the role of an attacker with a low, moderate, or high (AOV_VLA.2, AOV_VLA.3, or AOV_VLA.4, respectively) attack potential. Any exploitation of operational system vulnerabilities by such an attacker should be considered by the evaluator to be “obvious penetration attacks” (with respect to AOV_VLA.*.2C elements) in the context of the components AOV_VLA.2 through AOV_VLA.4.

C.8.3.3 Component levelling

This family contains four components. The components in this family are levelled on the basis of confirmation of developer/integrator analysis and depth of independent analysis.

C.8.3.4 AOV_VLA.1 Developer/integrator vulnerability analysis

Dependencies: ASD_IFS.1 Interface functional specification

ASD_SSD.1 Subsystem design

ASD_CON.1 Security concept of operations

AOD_ADM.1 Administrator guidance

AOD_USR.1 User guidance

C.8.3.4.1 Objectives

A vulnerability analysis is performed by the developer/integrator to ascertain the presence of obvious vulnerabilities, and to confirm that they cannot be exploited in the intended environment for the STOE.

C.8.3.4.2 Application notes

The evaluator should consider performing additional tests as a result of potential exploitable vulnerabilities identified during other parts of the evaluation.

C.8.3.4.3 Developer/integrator action elements

AOV_VLA.1.1D The developer/integrator shall perform and document an analysis of the STOE deliverables searching for obvious ways in which a user can violate the security enforcing functionality.

AOV_VLA.1.2D The developer/integrator shall document the disposition of obvious vulnerabilities.

C.8.3.4.4 Content and presentation of evidence elements

AOV_VLA.1.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the STOE.

C.8.3.4.5 Evaluator action elements

AOV_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOV_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer/integrator vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

C.8.3.5 AOV_VLA.2 Independent vulnerability analysis

Hierarchical to: AOV_VLA.1 Developer/integrator vulnerability analysis

Dependencies: ASD_IFS.1 Interface functional specification

ASD_SSD.1 Subsystem design

ASD_IMP.1 Implementation representation

ASD_CON.1 Security concept of operations

AOD_USR.1 User guidance

AOD_ADM.1 Administrator guidance

C.8.3.5.1 Objectives

A vulnerability analysis is performed by the developer/integrator to ascertain the presence of security vulnerabilities, and to confirm that they cannot be exploited in the intended environment for the STOE.

The evaluator performs independent penetration testing, supported by the evaluator's independent vulnerability analysis, to determine that the STOE is resistant to penetration attacks performed by attackers possessing a low attack potential.

C.8.3.5.2 Developer/integrator action elements

AOV_VLA.2.1D The developer/integrator shall perform and document an analysis of the STOE deliverables searching for **ways** in which a user can violate the security enforcing functionality.

AOV_VLA.2.2D The developer/integrator shall document the disposition of identified vulnerabilities.

C.8.3.5.3 Content and presentation of evidence elements

AOV_VLA.2.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the STOE.

AOV_VLA.2.2C The documentation shall justify that the STOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

C.8.3.5.4 Evaluator action elements

AOV_VLA.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOV_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer/integrator vulnerability analysis, to ensure **the identified** vulnerabilities have been addressed.

AOV_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.

AOV_VLA.2.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AOV_VLA.2.5E The evaluator shall determine that the STOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

C.8.3.6 AOV_VLA.3 Moderately resistant

Hierarchical to: AOV_VLA.2 Independent vulnerability analysis

Dependencies: ASD_IFS.1 Interface functional specification

ASD_SSD.1 Subsystem design

ASD_IMP.1 Implementation representation

ASD_CON.1 Security concept of operations

AOD_USR.1 User guidance

AOD_ADM.1 Administrator guidance

C.8.3.6.1 Objectives

A vulnerability analysis is performed by the developer/integrator to ascertain the presence of security vulnerabilities, and to confirm that they cannot be exploited in the intended environment for the STOE.

The evaluator performs independent penetration testing, supported by the evaluator's independent vulnerability analysis, to determine that the STOE is resistant to penetration attacks performed by attackers possessing a moderate attack potential.

C.8.3.6.2 Developer/integrator action elements

AOV_VLA.3.1D The developer/integrator shall perform and document an analysis of the STOE deliverables searching for ways in which a user can violate the security enforcing functionality.

AOV_VLA.3.2D The developer/integrator shall document the disposition of identified vulnerabilities.

C.8.3.6.3 Content and presentation of evidence elements

AOV_VLA.3.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the STOE.

AOV_VLA.3.2C The documentation shall justify that the STOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AOV_VLA.3.3C The evidence shall show that the search for vulnerabilities is systematic.

C.8.3.6.4 Evaluator action elements

AOV_VLA.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOV_VLA.3.2E The evaluator shall conduct penetration testing, building on the developer/integrator vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AOV_VLA.3.3E The evaluator shall perform an independent vulnerability analysis.

AOV_VLA.3.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AOV_VLA.3.5E The evaluator shall determine that the STOE is resistant to penetration attacks performed by an attacker possessing a **moderate** attack potential.

C.8.3.7 AOV_VLA.4 Highly resistant

Hierarchical to: AOV_VLA.3 Moderately resistant

Dependencies: ASD_IFS.1 Interface functional specification

ASD_SSD.1 Subsystem design

ASD_IMP.1 Implementation representation

ASD_CON.1 Security concept of operations

AOD_USR.1 User guidance

AOD_ADM.1 Administrator guidance

C.8.3.7.1 Objectives

A vulnerability analysis is performed by the developer/integrator to ascertain the presence of security vulnerabilities, and to confirm that they cannot be exploited in the intended environment for the STOE.

The evaluator performs independent penetration testing, supported by the evaluator's independent vulnerability analysis, to determine that the STOE is resistant to penetration attacks performed by attackers possessing a high attack potential.

C.8.3.7.2 Developer/integrator action elements

AOV_VLA.4.1D The developer/integrator shall perform and document an analysis of the STOE deliverables searching for ways in which a user can violate the security enforcing functionality.

AOV_VLA.4.2D The developer/integrator shall document the disposition of identified vulnerabilities.

C.8.3.7.3 Content and presentation of evidence elements

AOV_VLA.4.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the STOE.

AOV_VLA.4.2C The documentation shall justify that the STOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AOV_VLA.4.3C The evidence shall show that the search for vulnerabilities is systematic.

AOV_VLA.4.4C The analysis documentation shall provide a justification that the analysis completely addresses the STOE deliverables.

C.8.3.7.4 Evaluator action elements

AOV_VLA.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOV_VLA.4.2E The evaluator shall conduct penetration testing, building on the developer/integrator vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AOV_VLA.4.3E The evaluator shall perform an independent vulnerability analysis.

AOV_VLA.4.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AOV_VLA.4.5E The evaluator shall determine that the STOE is resistant to penetration attacks performed by an attacker possessing a **high** attack potential.

C.9 Class AOL: Operational system life cycle support

C.9.1 Introduction

The purpose of the life-cycle support is to judge the adequacy of the procedures used during the integration and operational life-cycles of the operational system. These procedures include the security measures used throughout operational system development (i.e., integration), the life-cycle model used by the integrator, and the tools used by the integrator throughout the life-cycle of the operational system.

C.9.2 Identification of operational system security measures (AOL_DVS)

C.9.2.1 Objectives

This family provides a means to provide the security measures during development of the operation system. The development activities should require confidentiality and integrity for development materials.

C.9.2.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.9.2.3 AOL_DVS.1 Identification of security measures

Dependencies: no dependencies.

C.9.2.3.1 Developer/integrator action elements

AOL_DVS.1.1D The developer/integrator shall produce development security documentation.

C.9.2.3.2 Content and presentation of evidence elements

AOL_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality, authenticity, reliability and integrity of the STOE design and implementation in its development and integration environment.

AOL_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the STOE.

C.9.2.3.3 Evaluator action elements

AOL_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.9.2.4 AOL_DVS.2 Verification of security measures

Hierarchical to: AOL_DVS.1 Identification of security measures

Dependencies: no dependencies.

C.9.2.4.1 Developer/integrator action elements

AOL_DVS.2.1D The developer/integrator shall produce development security documentation.

C.9.2.4.2 Content and presentation of evidence elements

AOL_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality, authenticity, reliability and integrity of the STOE design and implementation in its development and integration environment.

AOL_DVS.2.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the STOE.

C.9.2.4.3 Evaluator action elements

AOL_DVS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AOL_DVS.2.2E The evaluator shall independently verify through [selection: *personnel interviews, sampling the security measures*, [assignment: *other methods*]] that the security measures are being applied.

C.10 Class ASI: System security installation and delivery

C.10.1 Introduction

During installation it is necessary to establish and define the security management structure whose purpose is to promulgate and instil security policy and awareness into the organization. Management should visibly promote and support security within the organization through active participation in the implementation of security across the organization. Management activity includes articulating security goals to meet the organizational requirements, and is integrated in relevant business processes. Activities include formulating, reviewing, and approving security policy, ensuring that there is clear and visible management support, and providing security training and awareness programs in support of organizational security policy. It also designates a manager as the organization's security authority.

It is also necessary to confirm the adequacy of the procedures used to configure the operational system, both on installation and on routine start-up.

C.10.2 Awareness training (ASI_AWA)

C.10.2.1 Objectives

This family requires that the management provide training as a means for personnel to learn their security roles and responsibilities for conducting their business within the operational system.

C.10.2.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.10.2.3 ASI_AWA.1 Awareness training

Dependencies: no dependencies.

C.10.2.3.1 Management action elements

ASI_AWA.1.1M The management shall conduct awareness training with a formal induction process designed to introduce [selection: *all operational controls*, [assignment: *operational controls*]] and their expectation [selection: *before, within* [assignment: *time frame*], *periodically* [assignment: *time period*]] giving personnel access to the operational system assets.

C.10.2.3.2 Content and presentation of evidence elements

ASI_AWA.1.1C The awareness training shall be recorded.

ASI_AWA.1.2C The records shall contain date and time, authorized personnel, targeted personnel, contents and results of the training.

C.10.2.3.3 Evaluator action elements

ASI_AWA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.10.2.4 ASI_AWA.2 Verification of awareness training

Hierarchical to: ASI_AWA.1 Awareness training

Dependencies no dependencies.

C.10.2.4.1 Management action elements

ASI_AWA.2.1M The management shall conduct awareness training with a formal induction process designed to introduce [selection: *all operational controls*, [assignment: *operational controls*]] and their expectation [selection: *before, within* [assignment: *time frame*], *periodically* [assignment: *time period*]] giving personnel access to the operational system assets.

C.10.2.4.2 Content and presentation of evidence elements

ASI_AWA.2.1C The awareness training shall be recorded.

ASI_AWA.2.2C The records shall contain date and time, authorized personnel, targeted personnel, contents and results of the training.

C.10.2.4.3 Evaluator action elements

ASI_AWA.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASI_AWA.2.2E The evaluator shall independently verify through [selection: *personnel interviews, sampling the awareness training*, [assignment: *other methods*]] the veracity of conducting the awareness training.

C.10.3 Communication (ASI_CMM)

C.10.3.1 Objectives

This family requires that the management has some means of communicating operational guidance documentations that define and specify SSFs to the appropriate personnel.

C.10.3.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.10.3.3 ASI_CMM.1 Information on controls

Dependencies: no dependencies.

C.10.3.3.1 Management action elements

ASI_CMM.1.1M The management shall communicate [selection: *all SSFs*, [assignment: SSFs]] to all personnel associated with operational controls before giving them access to operational system assets.

C.10.3.3.2 Content and presentation of evidence elements

ASI_CMM.1.1C The information shall be recorded.

ASI_CMM.1.2C The records shall contain date and time, authorized personnel, targeted personnel and contents of the information.

C.10.3.3.3 Evaluator action elements

ASI_CMM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.10.3.4 ASI_CMM.2 Verification of information on controls

Hierarchical to: ASI_CMM.1 Information on controls

Dependencies: no dependencies.

C.10.3.4.1 Management action elements

ASI_CMM.2.1M The management shall communicate [selection: *all SSFs*, [assignment: SSFs]] to all personnel associated with operational controls before giving them access to operational system assets.

C.10.3.4.2 Content and presentation of evidence elements

ASI_CMM.2.1C The information shall be recorded.

ASI_CMM.2.2C The records shall contain date and time, authorized personnel, targeted personnel and contents of the information.

C.10.3.4.3 Evaluator action elements

ASI_CMM.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASI_CMM.2.2E The evaluator shall independently verify through [selection: *personnel interviews, sampling the operational controls*, [assignment: *other methods*]] the veracity of the communication of the operational controls.

C.10.4 Secure installation check (ASI_SIC)

C.10.4.1 Objectives

This family provides a means to verify the installation and start up of the STOE. The installation and start up of the STOE should be implemented and operated correctly and effectively in accordance with the security policy of the operational system.

C.10.4.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.10.4.3 ASI_SIC.1 Secure installation check

Dependencies: no dependencies.

C.10.4.3.1 Management action elements

ASI_SIC.1.1M The developer/integrator shall document secure installation procedures necessary to ensure that components and interfaces that comprise the STOE, especially those to legacy security controls and interfaces, can be installed, started up and interoperate in a secure manner.

C.10.4.3.2 Content and presentation of evidence elements

ASI_SIC.1.1C The secure installation procedures documentation shall describe the steps necessary for verification of secure installation, start-up and interoperation of the STOE in its environment.

C.10.4.3.3 Evaluator action elements

ASI_SIC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.10.4.4 ASI_SIC.2 Verification of secure installation check

Hierarchical to: ASI_SIC.1 Secure installation check

Dependencies: no dependencies.

C.10.4.4.1 Management action elements

ASI_SIC.2.1M The developer/integrator shall document secure installation procedures necessary to ensure that components and interfaces that comprise the STOE, especially those to legacy security controls and interfaces, can be installed, started up and interoperate in a secure manner.

C.10.4.4.2 Content and presentation of evidence elements

ASI_SIC.2.1C The secure installation procedures documentation shall describe the steps necessary for verification of secure installation, start-up and interoperation of the STOE in its environment.

C.10.4.4.3 Evaluator action elements

ASI_SIC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASI_SIC.2.2E The evaluator shall verify that the secure installation procedures result in a secure configuration.

C.11 Class ASO: Records on operational system

C.11.1 Introduction

Operational system may be under changing and modification always. Changes and modifications would include changes requests, service packs, any applied software patches and specialized interoperability or compatibility requirements driven by the addition of, or change to an existing internal or external interface.

This class contains families that govern how SSFs are conducting correctly and effectively during operation of the system. The primary purpose of operation of system security is to enable a determination that the operational system is operating in a secure manner without violation of operational system security policies. It also defines actions that will take place if and when security relevant events occur. This class ensures that appropriate actions are taken to detect, record and respond to events that may be possible violations of the operational system security policy.

The families in this class define a means for management to monitor and verify the operational controls.

C.11.2 Operation records of operational controls (ASO_RCD)

C.11.2.1 Objectives

This family provides operation records for the SSFs during the operation. The operational controls should be implemented and operated correctly and effectively in accordance with the security policy of the operational system.

C.11.2.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.11.2.3 ASO_RCD.1 Record of operational controls

Dependencies: no dependencies.

C.11.2.3.1 Management action elements

ASO_RCD.1.1M The management shall record the operational evidence defined by [selection: *all operational controls* or [assignment: *operational controls*]].

C.11.2.3.2 Content and presentation of evidence elements

ASO_RCD.1.1C The information associated with the operational evidence shall be recorded.

ASO_RCD.1.2C The records shall contain date and time, responsible person, targeted operational controls and results of the operation.

C.11.2.3.3 Evaluator action elements

ASO_RCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.11.2.4 ASO_RCD.2 Verification of operational records

Hierarchical to: ASO_RCD.1 Record of operational controls

Dependencies: no dependencies.

C.11.2.4.1 Management action elements

ASO_RCD.2.1M The management shall record the operational evidence defined by [selection: *all operational controls* or [assignment: *operational controls*]].

C.11.2.4.2 Content and presentation of evidence elements

ASO_RCD.2.1C The information associated with the operational evidence shall be recorded.

ASO_RCD.2.2C The records shall contain date and time, responsible person, targeted operational controls and results of the operation.

C.11.2.4.3 Evaluator action elements

ASO_RCD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASO_RCD.2.2E The evaluator shall independently verify through [selection: *personnel interviews, sampling the operational records*, [assignment: *other methods*]] that the information concerning operation of operational controls is being correctly recorded.

C.11.3 Verification of operational controls (ASO_VER)

C.11.3.1 Objectives

This family provides a means to verify the operational controls during the operation. The operational controls should be implemented and operated correctly and effectively in accordance with the security policy of the operational system.

C.11.3.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.11.3.3 ASO_VER.1 Verification of operational controls

Dependencies: no dependencies.

C.11.3.3.1 Management action elements

ASO_VER.1.1M The management shall verify that [selection: *all operational controls* or [assignment: *operational controls*]] are installed and operated correctly and effectively.

C.11.3.3.2 Content and presentation of evidence elements

ASO_VER.1.1C The information associated with the verification shall be recorded.

ASO_VER.1.2C The records shall contain date and time, responsible person, targeted operational controls and results of the verification.

C.11.3.3.3 Evaluator action elements

ASO_VER.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.11.3.4 ASO_VER.2 Independent verification of operational controls

Hierarchical to: ASO_VER.1 Verification of operational controls

Dependencies: no dependencies.

C.11.3.4.1 Management action elements

ASO_VER.2.1M The management shall verify that [selection: *all operational controls* or [assignment: *operational controls*]] are installed and operated correctly and effectively.

C.11.3.4.2 Content and presentation of evidence elements

ASO_VER.2.1C The information associated with the verification shall be recorded.

ASO_VER.2.2C The records shall contain date and time, responsible person, targeted operational controls and results of the verification.

C.11.3.4.3 Evaluator action elements

ASO_VER.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASO_VER.2.2E The evaluator shall independently verify through [selection: *personnel interviews, sampling the operational controls*, [assignment: *other methods*]] that the operational controls are installed and operated correctly and effectively.

C.11.4 Monitoring of operational controls (ASO_MON)

C.11.4.1 Objectives

This family provides a means to monitor the operational controls during the operation. The primary purpose of operational control monitoring is to enable a determination that operational controls are operating in a secure manner without violation of operational system security policies. The operational controls should be implemented and operated correctly and effectively in accordance with the security policy of the operational system. It also defines actions that will take place if and when some changes occur in the operational systems.

C.11.4.2 Component levelling

This family contains two components. The components in this family are levelled on the basis of confirmation of description in the documentation and verification in the operational system.

C.11.4.3 ASO_MON.1 Monitoring of operational controls by management

Dependencies: no dependencies.

C.11.4.3.1 Management action elements

ASO_MON.1.1M The management shall monitor the provisions and performance levels of [selection: *all operational controls* or [assignment: *operational controls*]] at regular period.

ASO_MON.1.2M The management shall monitor the changes to provision of services including maintenance and improvement of security policies, procedures and controls, taking account of criticality of business systems and processes involved and re-assessment of risks.

C.11.4.3.2 Content and presentation of evidence elements

ASO_MON.1.1C The information associated with the monitoring shall be recorded.

ASO_MON.1.2C The records shall contain date and time, responsible person, targeted operational controls and results of the monitoring.

C.11.4.3.3 Evaluator action elements

ASO_MON.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.11.4.4 ASO_MON.2 Verification of monitoring of operational controls

Hierarchical to: ASO_MON.1 Monitoring of operational controls by management

Dependencies: no dependencies.

C.11.4.4.1 Management action elements

ASO_MON.2.1M The management shall monitor the provisions and performance levels of [selection: *all operational controls* or [assignment: *operational controls*]] at regular period.

ASO_MON.2.2M The management shall monitor the changes to provision of services including maintenance and improvement of security policies, procedures and controls, taking account of criticality of business systems and processes involved and re-assessment of risks.

C.11.4.4.2 Content and presentation of evidence elements

ASO_MON.2.1C The information associated with the monitoring shall be recorded.

ASO_MON.2.2C The records shall contain date and time, responsible person, targeted operational controls and results of the monitoring.

C.11.4.4.3 Evaluator action elements

ASO_MON.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASO_MON.2.2E The evaluator shall independently verify through [selection: *personnel interviews, sampling the changes*, [assignment: *other methods*]] that the monitoring is conducted in accordance with the security policy.

Annex D
(informative)

Relationship to Common Criteria development

This annex identifies the necessary differences between the criteria for evaluation of operational systems and the criteria within the draft for comment Version 3.0 of the Common Criteria [10]. It also identifies where revision of this Technical Report would be appropriate if the changes in that document are propagated into a new version of ISO/IEC 15408.

There is nothing in the body of this Technical Report which is criteria version specific, and it is likely that no changes would be required following revision of ISO/IEC 15408 in line with [10].

Annex A of this Technical Report defines the layout and content of SPPs and SSTs. Annex A was prepared with knowledge of the proposed changes to the layout and content of ISO/IEC 15408 PPs and STs within [10] in mind, and adopts those proposed changes where appropriate. There is one major difference between the structures used for operational system evaluation and those proposed in [10], which is the capability to evaluate domain-specific requirements and controls. This is an intentional difference, and would remain following revision of ISO/IEC 15408 in line with [10].

Annex B of this Technical Report deals with operational system functional requirements. It is structured differently to ISO/IEC 15408, being based on structures adapted from NIST SP 800-53 [5] and ISO/IEC 17799 [4]. Thus the major changes to functional requirements between ISO/IEC 15408 and [10] have no impact on the text of this Technical Report; the new components for technical controls would be automatically included by updated reference. For compatibility with the terminology of [10], the name of the Annex should change to “operational system functional components”.

Annex C of this Technical Report addresses operational system assurance requirements. It defines nine new classes of assurance requirements. Some of these are innovative, other classes or families are based on ISO/IEC 15408 classes or families. It is therefore necessary to consider each family individually. For compatibility with the terminology of [10], the name of the Annex should change to “operational system assurance components”.

Class ASP of Annex C deals with SPP evaluation and resembles class APE of [10]. Family ASP_INT has differences relating to the relationship with external operational systems and the need to specify the domain organisation. There is no reference to non-TOE hardware and firmware, as this would form part of the operational system in all cases. There are two layered components depending on the degree of information provided concerning security objectives for each domain. Family ASP_CCL has no conformance type conformance claim, as system protection profiles cover all aspects of the associated operational systems. Family ASP_SPD deals with risks not threats, and does not permit assumptions about the operational environment since this is part of the evaluated operational system. Family ASP_OBJ permits objectives for external operational systems, but not for the operational environment since this is part of the evaluated operational system. It therefore has only one component. Family ASP_REQ permits external operational systems to meet objectives. There are multiple additional families dealing with domain specific requirements. These are all intentional differences, and would remain following revision of ISO/IEC 15408 in line with [10]. There are a number of minor differences, such as consistency checking of security problem definitions and objectives, which may represent problems within [10].

Class ASS of Annex C deals with SST evaluation and resembles class ASE of [10]. The differences are similar to those for ASP and APE for protection profiles. Family ASS_INT has differences relating to the relationship with external operational systems and the need to specify the domain organisation and their development environments. There is no reference to non-TOE hardware and firmware, as this would form part of the operational system in all cases. There are two layered components depending on the degree of information provided concerning security objectives for each domain. Family ASP_SPD deals with risks not threats, and does not permit assumptions about the operational environment since this is part of the evaluated operational system. Family ASP_OBJ permits objectives for external operational systems, but not for the

operational environment since this is part of the evaluated operational system. It therefore has only one component. Family ASP_REQ permits external operational systems to meet objectives. Family ASE_TSS asks for details of how assurance requirements are satisfied. This is necessary as different domains may meet the requirements in different ways. There are multiple additional families dealing with domain specific requirements. These are all intentional differences, and would remain following revision of ISO/IEC 15408 in line with [10]. There are a number of minor differences, such as checking that operations within requirements are completed consistently with PP restrictions, which may represent problems within [10].

Class AOD of Annex C deals with guidance documentation. Families AOD_OCD and AOD_GVR are unique to operational system evaluation. However, families AOD_ADM and AOD_USR are based on AGD_ADM and AGD_USR of ISO/IEC 15408. In [10], these are replaced by a single family AGD_OPE. A similar reorganisation would be needed for operational systems. This would generate minor changes to AOD_GVR in consequence.

Class ASD of Annex C deals with system architecture and design. It is based on the ISO/IEC 15408 ADV class, but with significant changes to deal with the additional information known about operational systems and their internal structure. Family ASD_SAD has no ISO/IEC 15408 equivalent, but is covered by part of the new family ADV_TDS of [10]. Family ASD_IFS is based on ADV_FSP, but limited to interface specifications as other security properties are examined through the various layers of design documentation. ASD_HLD is based on ADV_SSD, ASD_CMP on ADV_LLD and ASD_IMP on ADV_IMP, but in all cases extended to cover all aspects of the operational system and with a single level of information. Finally, family ASD_CON is new, identical in intent to the new family ADV_ARC of [10].

The mapping between the ADV class of ISO/IEC 15408 and the ADV class of [10] is extremely complex. Propagating the changes to this Technical Report would require complete reworking of the current ASD class.

Configuration management class AOC of Annex C is an addition, rather than replacement, to the ISO/IEC 15408 ACM class. Family AOC_OBM deals with operational configuration management. Families AOC_ECP, AOC_PPC and AOC_NCP deal with assurance from bought-in products. In [10], the ACM class has been absorbed into the ALC class. Component ALC.CMC.5, Advanced support, implements a restricted form of AOC_OBM. However, AOC_OBM is more general, and would still be needed, together with the rest of the AOC class, following revision of ISO/IEC 15408 in line with [10].

The testing class AOT of Annex C is closely based on the ISO/IEC 15408 ATE class, with an extra family AOT_REG to handle regression testing during system operation. AOT_FUN is derived from ATE_FUN, with extra requirements for integrated controls testing, and only one level as ordered testing is considered essential for operational systems. AOT_COV is derived from ATE_COV, with minor changes for different documentation requirements and no equivalent to level ATE.COV.1. AOT_DPT is derived from ATE_DPT, with minor changes due to different documentation requirements. The same applies to AOT_IND, derived from ATE_IND. In [10], all these four families are essentially unchanged. Some requirements have been changed to clarify their intended meaning. Some documentation deliverables have different names. Following revision of ISO/IEC 15408 in line with [10], these editorial changes would need to be carried across. The additional AOT_REG family would remain unchanged.

Class AOV of Annex C deals with vulnerability analysis. It is derived from some families of the ISO/IEC AVA class. There is no equivalent of AVA_SOF, as operational controls are extremely unlikely to be realised by probabilistic or permutational mechanisms. Similarly, there is no equivalent to AVA_CCA, as covert channels are extremely unlikely to be implemented through side-effects of operational controls. Family AOV_MSU is based on AVA_MSU, but without an equivalent to lowest level AVA_MSU.1. AOV_MSU addresses the misuse of operational controls rather than the operational environment assumptions of AVA_MSU. In [10], AVA_MSU has been merged into the AGD class. The same approach could be used in operational systems. The final family, AOV_VLA, is based on AVA_VLA, but restructured to make the purpose of vulnerability analysis explicit. In [10], the equivalent family, AVA_VAN, has a radically changed approach – it moves responsibility for vulnerability analysis onto the evaluator and increases the number of levels as compared to AVA_VLA. This new philosophy would need to be carried across to AOV_VLA, with mainly editorial changes to handle different documentation deliverables.

The life cycle support class AOL of Annex C contains a single family AOL_DVS, dealing with security measures to protect the development environment. This family is almost identical to the ALC_DVS class of [10], much closer to that version than the ALC_DVS family of ISO/IEC 15408. Because it deals only with development environment security, it is probable that following revision of ISO/IEC 15408 in line with [10], it could be withdrawn, to be replaced by use of the revised version of ADV_DVS.

The two final classes ASI and ASO of Annex C deal with operational controls during system installation and operation respectively. These are new and unrelated to any ISO/IEC 15408 classes, and it is therefore likely that no changes would be needed following revision of ISO/IEC 15408 in line with [10].

Bibliography

[1] ISO/IEC 13335 (all parts), *Information technology — Security techniques — Management of information and communications technology security*

NOTE ISO/IEC 13335 is being replaced by standards in the ISO/IEC 27000 family of standards.

[2] *Guide for the Security Certification and Accreditation of Federal Information Systems*, NIST Special Publication SP 800-37, Department of Commerce, United States

[3] ISO/IEC TR 15443 (all parts), *Information technology — Security techniques — A framework for IT security assurance*

[4] ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

[5] *Recommended Security Controls for Federal Information Systems*, NIST Special Publication SP 800-53, Second Public Draft, September 2004, Department of Commerce, United States

[6] ISO/IEC 21827, *Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)*

[7] ISO/IEC TR 15446, *Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets*

[8] *Guide for Assessing the Security Controls in Federal Information Systems*, NIST Special Publication SP 800-53A, Department of Commerce, United States (not yet available)

[9] *IT Baseline Protection Manual*, Bundesamt für Sicherheit in der Informationstechnik, Germany. ISBN 3-88784-915-9

[10] *Common Criteria for Information Technology Security Evaluation*, Version 3.0, Revision 2, June 2005, Common Criteria Development Board

ICS 35.040

Price based on 165 pages