E C M A

EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

STANDARD ECMA - 205

Commercially oriented functionality class for security evaluation (COFC)

December 1993

Free copies of this document are available from ECMA,
European Computer Manufacturers Association,
114 Rue du Rhône - CH-1204 Geneva (Switzerland)

Phone: +41 22 735 36 34 Fax: +41 22 786 52 31
X.400: C=ch, A=arcom, P=ecma, O=genevanet,
OU1=ecma, S=helpdesk
Internet: helpdesk@ecma.ch

E C M A

EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

STANDARD ECMA - 205

Commercially oriented functionality class for security evaluation (COFC)

December 1993

Brief History

In September 1990 the European Commission announced the "Harmonized IT Security Evaluation Criteria" ITSEC. The governments of France, Germany, Great Britain and the Netherlands had agreed on a common set of criteria for IT security evaluations. The European Commission proposed these criteria for usage within the European Community.

The ITSEC deviated substantially from the US TCSEC, (Trusted Computer System Evaluation Criteria) commonly known as Orange Book, the de-facto standard since 1983.

This created a problem for all world-wide operating computer manufacturers who were faced with two problems:

- to which set of criteria they should develop their products, and
- if a product was developed to one set of criteria, would a customer in a country outside the influence of this set accept the product and its evaluation.

Users of IT products were confused because they did not know, which set of criteria would meet their requirements.

The European Computer Manufacturers Association, ECMA, was alerted by its members, mostly world-wide operating companies. The ECMA General Assembly therefore decided already in December 1990 to establish an ad hoc group on Security. This group started its work in March 1991. Later in 1991 the group became ECMA/TC36 and then TC36/TG1.

The group decided to address the problem twofold:

- First, to write an ECMA Technical Report which positions security evaluations in the context of secure information processing in order to highlight the fact that an evaluated product or system can only guarantee security, when the total system, its environment and its operation are secure.
- Second, to develop an ECMA Standard for a functionality class which defines a minimum set of requirements for commercial application. This class was called "Commercially Oriented Functionality Class" or COFC. It distinguishes itself from the Orange Book and respective ITSEC functionalities, which are more tuned towards military and government requirements for confidentiality of classified information. Assurance criteria, as addressed on the Orange Book and ITSEC, have not been taken into account.

Both, the Technical Report and the Standard are intended to be a contribution to the ongoing harmonisation process. They highlight commercial requirements, which call for an appropriate evaluation process, ranging from vendor self-testing to accredited third party testing, and a minimal set of functional requirements, which satisfy commercial needs.

This ECMA Standard has been adopted by the ECMA General Assembly of December 1993.

Table of contents

1 Scope

The objective of this ECMA Standard is to define a widely accepted basic security functionality class for the commercial market. It is articulated in a structured way consistent with TCSEC, ITSEC and MSFR concepts. Readers unfamiliar with security and these concepts are encouraged to read TCSEC, ITSEC and MSFR if they wish to understand fully this text.

This standard addresses only IT security. Other security areas like personnel security, physical security and procedural security are not covered.

This standard defines a basic functionality class for the commercial market. It addresses multi-user, stand-alone IT-systems without considering networking or remote access. The areas networking, distributed processing, anonymity, pseudonymity, unlinkability, unobservability are still evolving. Once these matters are better understood additional requirements will be defined as an add-on, in a new version of this class or in a new extended class. Multi-processor systems however are covered as long as a single system image is provided.

Table 1 shows the security enforcing functions by which the major assumed threats are countered.

Table 1. Major assumed threats countered by security enforcing functions

THREAT	SECURITY ENFORCING FUNCTION
Outsider attack - Unauthorized access to the TOE	6.1.2 Identification and Authentication prior to all other interactions
Insider attack - Individual responsibility	6.1.1 Unique Identification and Authentication 6.3 Accountability 6.4 Audit
Automatic logon attacks	6.1.5 Number of logon trials
Disclosure of authentication information	6.1.9 Authentication information protection 6.1.10 Authentication information sharing 6.1.11 Authentication information aging
Disclosure of information	6.2 Access Control 6.5 Object Reuse
Manipulation of information (accidental or intentional)	6.2 Access Control 6.6 Accuracy
TOE failure	6.7.1 Recovery
Natural disasters	6.7.2 Data backup

This Standard defines minimum functional requirements independent of any platform. It focuses on functions and not on mechanisms or implementation specific details. Where mechanisms are addressed, e.g. "Password specific requirements," they are clearly separated. Examples are introduced with the phrase "As an example ..."; they are for illustration purposes only.

2 Conformance

A system conforms to the requirements of this Standard if it conforms to clause 6, and if a password mechanism is available, to the requirements of clause 7.

To conform to this Standard, systems with functions not covered in this Standard, such as Networking or Remote Access, are required to counter all the threats addressed by this functionality class and may require significant additional security enforcing functions and definitions.

3 References

ECMA-138	Security in open Systems - Data Elements and Service Definitions (1989)
ECMA TR/46	Security in open Systems - A Security Framework (1988)
ECMA TR/64	Secure information processing versus the concept of product evaluation (1993)
ECMA-206	Association context management - Including security context management (1993)
ISO 7498-2:1989	Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.
ISO 9594-2:1990	Information technology - Open Systems Interconnection - The Directory - Part 2: Models - Annex F (Informative) Access Control.
CBEMA	The American National Dictionary for Information Processing Systems - Computer and Business Equipment Manufacturers Association (1982).
TCSEC	Trusted Computer System Evaluation Criteria (TCSEC) - Department of Defense - DoD 5200.28-STD (December 1985).
ITSEC	Information Technology Security Evaluation Criteria (ITSEC) - Provisional Harmonised Criteria - Commission of the European Communities - ISBN 92-826-3004-8 (June 1991).
MSFR	Minimum Security Functionality Requirements for Multi-user Operating Systems - National Institute of Standards and Technology - Issue 1 (January 16, 1992).

4 Definitions

4.1 Terms defined in this document

For the purpose of this document the following definitions apply:

4.1.1 Access right

The ability of a user to access an object.

4.1.2 Administration

The act of controlling security relevant objects. This can be performed by one or several users through the assignment of security relevant access rights.

NOTE
These users are sometimes called administrators.

4.1.3 Customer-specifiable

A characteristic of security relevant parameters for which a customer can specify a value.

4.1.4 Identification

The process of recognising a user by the TOE. This is done by the user providing the TOE with some information that is known by the TOE and associated with the user. [See ITSEC page 25]

4.1.5 User identifier

A string of characters that uniquely identifies a user to a system.

NOTE
This does not exclude a user which does have several identifiers within the system, for instance, as described in ECMA-138 and ECMA TR/46.

4.2 Terms defined in other documents

The following terms are used with the meanings defined in other documents. The definitions are repeated for convenience in annex B.

Access
Access Control
Access Control List
Accountability
Audit
Audit Trail
Authenticate
Authentication Information
Authorization
Availability
Confidentiality
Customer
Data Integrity
Integrity
Mechanism
Object
Object Reuse
Password
Procedure
Security
Security Audit
Security Audit Trail
Security Enforcing
Security Mechanism
Target of Evaluation (TOE)
User

5 Acronyms

The following acronyms are used in this document:

ACL	Access Control List
CBEMA	Computer and Business Equipment Manufacturers Association
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
MSFR	Minimum Security Functionality Requirements
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation [ITSEC]

6 Specification of security enforcing functions

6.1 Identification and Authentication

6.1.1 Unique Identification and Authentication

The TOE shall uniquely identify and authenticate users.

6.1.2 Identification and Authentication prior to all other interactions

Identification and Authentication shall take place prior to all other interactions between the TOE and the user. Other interactions shall only be possible after successful identification and authentication.

6.1.3 Associate information to users

A mechanism shall be available for administration to associate customer-defined information, e.g., user name and affiliation, with each user.

6.1.4 Logon message

The TOE shall provide an advisory warning message upon TOE entry regarding unauthorized use, and the possible consequences of failure to meet those requirements. The message shall be customer-specifiable to meet their own requirements and state laws.

6.1.5 Number of logon trials

The TOE logon procedure shall exit and end the session if the user authentication procedure is incorrectly performed a customer-specifiable number of times within a logon session.

– The TOE shall provide a mechanism to immediately notify administration when this threshold is exceeded.

– When the above threshold has been exceeded, a customer-specifiable interval of time shall elapse before the logon process can be restarted on that I/O port.
– The TOE shall not suspend the user upon exceeding the above threshold.

6.1.6 Expiration of unused user identifiers

The TOE shall allow the customer to specify an action which is taken by the TOE after a period of time during which the user was not logged on. The time period shall be customer-specifiable.

As an example the following actions may be provided:
– disabling the access of the user to the TOE;
– alerting administration.

6.1.7 Disable users temporarily

The TOE shall allow administration to temporarily disable a user accessing the TOE.

6.1.8 User status information

A mechanism shall be available for administration to provide the status, e.g., active, inactive, etc., of any user.

6.1.9 Authentication information protection

The TOE shall protect the integrity of stored authentication information and the confidentiality of any associated secrets.

6.1.10 Authentication information independence

User-provided authentication information need not be unique. For example, two users may provide the same password, however the TOE shall not indicate the presence or absence of such duplicated authentication information.

6.1.11 Authentication information aging

If the authentication information is not biometric the TOE shall provide a mechanism which enforces periodic changes. The time period shall be customer-specifiable.

6.2 Access Control

6.2.1 Authenticated user identification

Control of access to objects shall only be granted to authenticated users, e.g. through an authenticated user identifier.

6.2.2 Individual user

The TOE shall be able to distinguish and administer access rights between each user and the objects which are subject to the administration of access rights. It shall be possible to grant the access rights down to the granularity of an individual user.

6.2.3 User groups

The TOE shall be able to distinguish and administer access rights between each user group and the objects which are subject to the administration of access rights, on the basis of membership to a group of users. It shall be possible to grant the access rights down to the granularity of an individual group.

6.2.4 Objects

Distinct security relevant objects shall be subject to the administration of access rights.

As an example the following objects may be subject to the administration of access rights:

– The objects of one user to protect them from any other user and their objects.
– The objects of the TOE (security relevant objects) to protect them from any user and their objects.

To allow functional separation of administrative users it shall be possible to grant access rights to individual security relevant objects to different users.

As an example the following security relevant objects may be subject to the administration of access rights:

– The Identification and Authentication mechanisms objects.
– The Access Control mechanisms objects.

- The Accountability mechanisms objects for non-administrative tasks.
- The Accountability mechanisms objects for administrative tasks.
- The Audit mechanisms objects.

6.2.5 Types of access rights

The TOE shall support at least these access right types:

1. Read: Allows to read but not to modify a protected object.
2. Modify: Allows to read and to modify a protected object.

6.2.6 Default access rights

The TOE shall provide a mechanism to specify default access rights for users not otherwise specified either explicitly or implicitly by group membership.

6.2.7 Precedence of access rights

The precedence rules shall be clear and unambiguous.

As an example the following rules are provided:

- The access rights associated with an individual user take precedence over the access rights associated with any group of which that user is a member.
- The access rights associated with any group of which a user is a member take precedence over any default access rights for that user.
- For TOEs where a user can be a member of multiple groups simultaneously, if any group entry allows an access right for that user, then the user is allowed that right.

6.2.8 Date of modification

The TOE shall be able to provide the date and time of the last modification to objects which are subject to the administration of rights.

6.2.9 Verification of rights

With each attempt by users or user groups to access objects which are subject to the administration of rights, the TOE shall verify the validity of the request. Unauthorised access attempts shall be rejected.

6.2.10 Application controlled access rights

The TOE shall provide the capability to allow access to the TOE via specific customer-defined applications such that the applications' access control security policies take precedence over the access rights of the invoking user.

6.3 Accountability and audit

6.3.1 Associate actions and users

For every interaction the TOE shall be able to establish the identity of the user.

6.3.2 Logging

The TOE shall contain an accountability component which is able, for each of the events 6.3.2.1 to 6.3.2.4 to log that event together with the required data to provide sufficient information for after-the-fact investigation of loss or impropriety and for appropriate management response, which may include personnel actions and pursuit of legal remedies.

6.3.2.1 Use of the identification and authentication mechanism

The TOE shall log at least logons and security-related activities of administration.

Administration shall have the capability to enable or disable the logging of other events which include at a minimum:

1. Valid and invalid user authentication attempts.

6.3.2.2 Actions that attempt to exercise access rights to an object which is subject to the administration of rights

The TOE shall log at least each of the following events:

1. Unsuccessful data or transaction access attempts.

Administration shall have the capability to enable or disable the logging of other events which include at a minimum:

1. Disk file access.
2. Tape volume or tape file access.
3. Program execution.
4. On-line execution of commands which are security relevant.

6.3.2.3 Creation or deletion of an object which is subject to the administration of rights

Administration shall have the capability to enable or disable the logging of other events which include at a minimum:

1. Creation and deletion of an object.

6.3.2.4 Actions by authorised users affecting the security of the TOE

The TOE shall log at least each of the following events:

1. Introduction or deletion (suspension) of users.
2. Introduction or removal of storage media.
3. Start up or shut down of the TOE.
4. Changes to user's security profiles, administration, or attributes.

6.3.2.5 Logged information

For each of the events 6.3.2.1 to 6.3.2.4 the TOE shall log the following information:

1. Date.
2. Time.
3. User identifier.
4. Type of event.
5. Name of the object.
6. Type of access attempt.
7. Success or failure of the attempt.

NOTE
For the use of the identification and authentication mechanism the object is the identifier of the equipment (e.g. terminal-id).
In case of start-up or shut-down, the object is the TOE. The name may be omitted.

6.3.3 TOE restart

Accountability control information shall survive restarts of the TOE.

6.3.4 Copy audit trails

The TOE shall provide a mechanism for automatic copying of audit trail files to a customer-specifiable storage medium after a customer-specifiable period of time.

6.3.5 Alarm if unable to record

The TOE shall allow site control of the procedure to be invoked when audit records are unable to be recorded.

The TOE shall generate an alarm to administration if audit records are unable to be recorded.

6.3.6 Select users

It shall be possible to selectively account for the actions of one or more users.

6.3.7 Dynamic control

Administration shall be able to dynamically display and modify the types of events recorded during normal TOE operation. This control shall include selective disabling of the recording of default audit events and the enabling and disabling of other optional events.

6.3.8 Audit tools

Tools to examine the audit trail for the purpose of audit shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively.

6.4 Object Reuse

The TOE shall be able to treat all returned storage objects before reuse by other users, in such a way that no conclusions can be drawn regarding the preceding content.

6.5 Accuracy

6.5.1 TOE software integrity

Procedures, e.g., use of modification dates, checksums, etc., shall exist that make it possible to verify that the currently installed TOE has remained consistent with the delivered software.

6.5.2 Data integrity

The TOE shall make available a mechanism to verify the integrity of data, e.g. checksum.

6.5.3 Security parameters status report

The TOE shall provide a mechanism for administration to generate a status report detailing the values of all customer-specifiable security parameters.

6.6 Reliability of service

6.6.1 Recovery

Procedures or mechanisms shall be provided to allow recovery after a TOE failure or other discontinuity.

6.6.2 Data backup

Procedures shall be provided for software and data backup and restoration.

7 Password specific requirements

This clause is applicable if a password mechanism is available within the TOE.

7.1 User-changeable password

The TOE shall provide a mechanism to allow passwords to be user-changeable. This mechanism shall require re-authentication of the user.

1. Administration shall have a mechanism to initialise passwords for users. A mechanism shall be provided to allow expiration upon their first use.
2. Password shall be stored in one-way encrypted form only.

7.2 Password aging

The TOE shall enforce password aging, i.e. a user's password shall be required to be changed after a customer-specifiable minimum time.

7.3 Password expiration notification

The TOE shall provide a mechanism to notify users in advance of requiring them to change their passwords. This can be done by either:

1. Notifying users a customer-specifiable period of time prior to their password expiring.
2. Upon password expiration, notifying the user but allowing a customer-specifiable subsequent number of additional usages prior to requiring a new password.

7.4 Password reuse

The TOE shall provide a mechanism to prohibit password reuse. This can be done by either:

1. Passwords shall not be reusable by the same individual for a customer-specifiable period of time or a number of password changes.
2. The user shall not be able to change the password again for a customer-specifiable period of time.

7.5 Password complexity

The TOE shall provide a method of ensuring the complexity of user-entered passwords that meets the following requirements:

1. Passwords shall meet a customer-specifiable minimum length requirement.
2. The password complexity-checking algorithm shall be modifiable by site.

7.6 Password logging

Plain text actual or attempted passwords shall not be displayed or logged.

7.7 Default passwords

During installation the TOE shall require default passwords to be changed.

Annex A

(informative)

Access control model

The purpose of this annex is to bridge the gap between the traditional way expressing access control as a combination of access rights and privileges (figure A.1) versus an object oriented view which would see these as a hierarchy of the same concept (figure A.2).

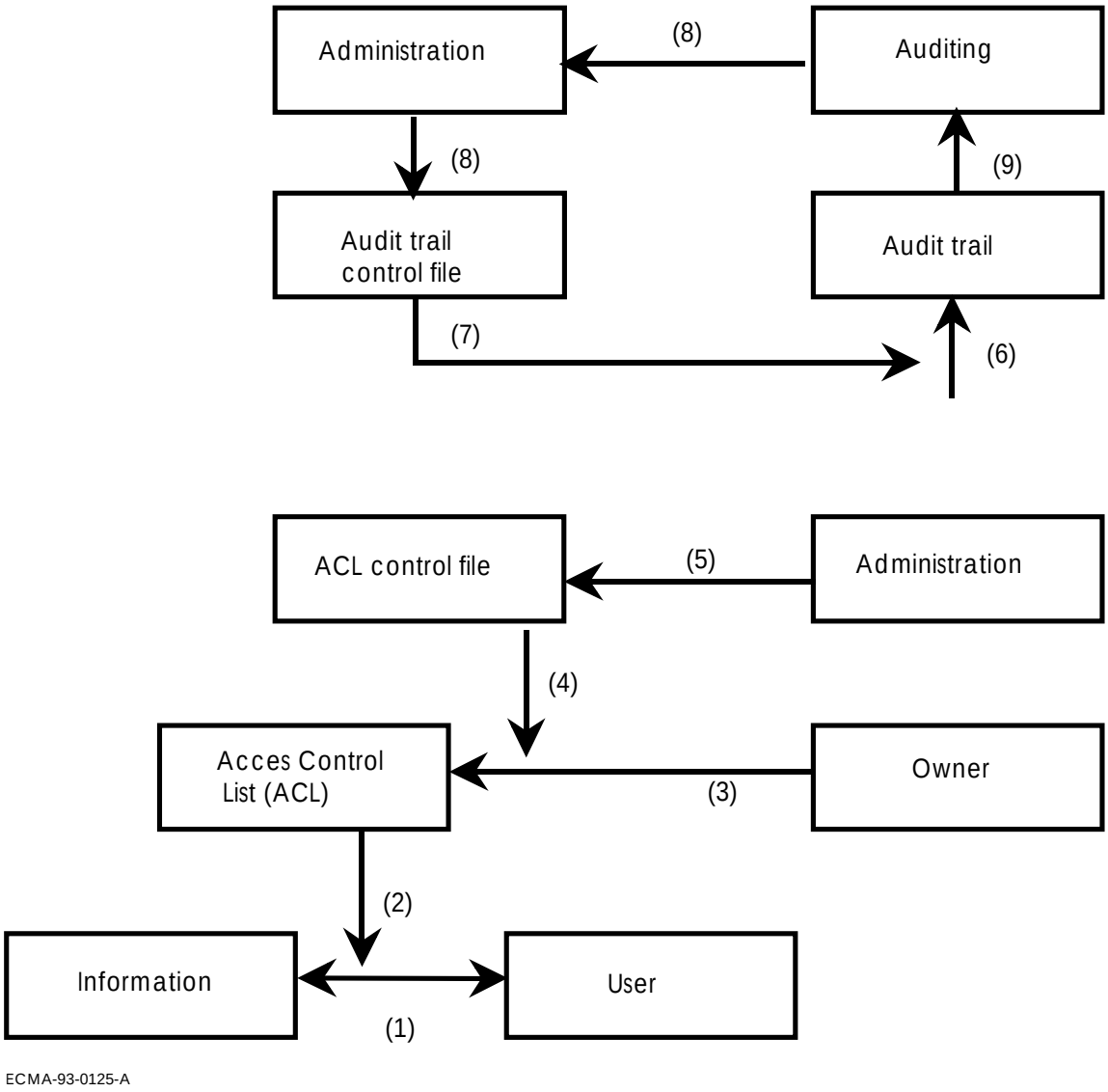

Figure A.1 - Example of access control and accountability

Figure A.1 is the scenario of a typical access control system. The user accesses information (1). Not every user has access to every information. Thus there is an Access Control List (ACL). It defines which user has which access rights to a specific piece of information (2). The ACL is set up by the owner of the information (3). In an ACL control file it is defined which rights an owner can grant (4). The ACL control file is managed by administration (5).

If there is also an accountability function certain events are recorded in an audit trail (6). In an audit trail control file it is defined which events are recorded (7). Auditing defines the audit trail control file (8) and exploits the audit trail (9).

NOTE
The term "audit trail" is defined in ISO 7498-2. But ITSEC use the term "accountability file" in the example functionality classes [ITSEC p. 124].

In traditional operating systems there is a distinction between access rights and privileges. Privileges may be defined as follows: "A privilege is the ability to exercise a controlled or restrictive service." Already in the simple scenario of figure A.1 it is difficult to define the exact border between access right and privilege. Is the ability of the user to modify the ACL (3) a privilege? Is it a lower privilege than the ability of the administrator to modify the ACL (4)? Or is the ability to modify the ACL control file (6) an ever higher privilege?

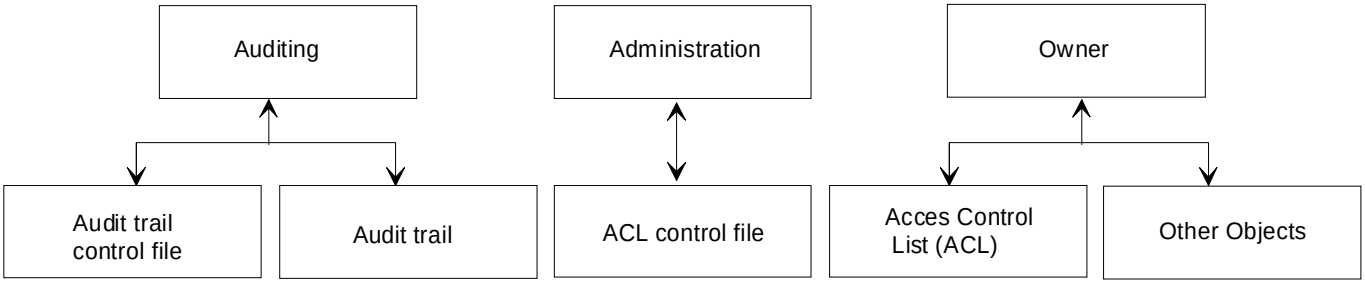

Figure A.2 - Example of access control and accountability in a flat model

To avoid these problems all information is called objects and seen at the same level as shown in figure A.2. In the same way the users are seen at the same level. There are just different users having different access rights to different objects. Some objects as well as some access rights are more security relevant than others.

The more granular the security relevant objects and access rights are the more granular the roles of individual administrative users can be defined to support the separation of responsibilities and mutual control.

In this ECMA Standard we have chosen the object oriented view. But this does not preclude an implementation with privileges.

Annex B

(informative)

Terms defined in other documents

The following terms are used with the meanings defined in the referenced documents. The definitions are repeated here for convenience.

Access: A specific type of interaction between a subject and an object that results in the flow of information from one to the other. [TCSEC].

Access control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. [ISO 7498-2].

Access control list: A list of entities, together with their access rights, which are authorized to have access to a resource. [ISO 7498-2].

Accountability: The property that ensures that the actions of an entity may be traced uniquely to the entity. [ISO 7498-2].

Audit: See Security Audit.

Audit trail: See Security Audit Trail.

Authenticate: To establish the validity of a claimed identity. [TCSEC].

Authentication information: Information used to establish the validity of a claimed identity. [ISO 7498-2].

Authorization: The granting of rights, which includes the granting of access based on access rights. [ISO 7498-2].

Availability: The property of being accessible and useable upon demand by an authorized entity. [ISO 7498-2].

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO 7498-2].

Customer: The person or organisation that purchases a Target of Evaluation. [ITSEC].

Data integrity: The property that data has not been altered or destroyed in an unauthorised manner. [ISO 7498-2].

Integrity: The prevention of unauthorised modification of information. [ITSEC]. See also Data Integrity.

Mechanism: See security mechanism.

Object: A passive entity that contains or receives information. [TCSEC, ITSEC].

Object reuse: The reassignment to some subject of a medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. [TCSEC]

Password: Confidential authentication information usually composed of a string of characters. [ISO 7498-2].

Procedure: The description of the course of action taken for the solution of a problem. [CBEMA].

Security: The combination of confidentiality, integrity and availability. [ITSEC].

Security audit: An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures. [ISO 7498-2].

Security audit trail: Data collected and potentially used to facilitate a security audit. [ISO 7498-2].

Security enforcing: That which directly contributes to satisfying the security objectives of the Target of Evaluation. [ITSEC].

Security mechanism: The logic or algorithm that implements a particular security enforcing or security relevant function in hardware or software. [ITSEC].

Target of evaluation (TOE): An IT system or product which is subject to security evaluation. [ITSEC].

User: Any person who interacts directly with a computer system. [TCSEC].