



INTERNATIONAL TELECOMMUNICATION UNION

**CCITT**

THE INTERNATIONAL  
TELEGRAPH AND TELEPHONE  
CONSULTATIVE COMMITTEE

**X.740**

(09/92)

**DATA COMMUNICATION NETWORKS**

---

**INFORMATION TECHNOLOGY –  
OPEN SYSTEMS INTERCONNECTION –  
SYSTEMS MANAGEMENT: SECURITY AUDIT  
TRAIL FUNCTION**



**Recommendation X.740**

---

## Foreword

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The CCITT (the International Telegraph and Telephone Consultative Committee) is a permanent organ of the ITU. Some 166 member countries, 68 telecom operating entities, 163 scientific and industrial organizations and 39 international organizations participate in CCITT which is the body which sets world telecommunications standards (Recommendations).

The approval of Recommendations by the members of CCITT is covered by the procedure laid down in CCITT Resolution No. 2 (Melbourne, 1988). In addition, the Plenary Assembly of CCITT, which meets every four years, approves Recommendations submitted to it and establishes the study programme for the following period.

In some areas of information technology, which fall within CCITT's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC. The text of CCITT Recommendation X.740 was approved on 10th September 1992. The identical text is also published as ISO/IEC International Standard 10164-8.

---

### CCITT NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication Administration and a recognized private operating agency.

© ITU 1993

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

# Contents

|         | <i>Page</i>  |
|---------|--|
| 1       | Scope..... 1   |
| 2       | Normative references ..... 1   |
| 2.1     | Identical Recommendations   International Standards ..... 2                              |
| 2.2     | Paired Recommendations   International Standards equivalent in technical content ..... 2 |
| 2.3     | Additional references ..... 3  |
| 3       | Definitions..... 3   |
| 3.1     | Basic reference model definitions..... 3   |
| 3.2     | Security architecture definitions ..... 3  |
| 3.3     | Management framework definitions ..... 3   |
| 3.4     | Systems management overview definitions ..... 3  |
| 3.5     | Event report management definitions ..... 4  |
| 3.6     | Security alarm reporting definitions..... 4  |
| 3.7     | Log control definitions..... 4   |
| 3.8     | OSI conformance testing definitions..... 4   |
| 4       | Abbreviations ..... 4  |
| 5       | Conventions..... 4   |
| 6       | Requirements..... 5  |
| 7       | Model ..... 5  |
| 8       | Generic definitions ..... 5  |
| 8.1     | Generic notifications..... 5   |
| 8.2     | Managed object..... 6  |
| 8.3     | Imported generic definitions ..... 7   |
| 8.4     | Compliance ..... 7   |
| 9       | Service definition ..... 7   |
| 9.1     | Introduction..... 7  |
| 9.2     | Security audit trail reporting service ..... 7   |
| 10      | Functional units..... 8  |
| 11      | Protocol ..... 8   |
| 11.1    | Elements of procedure ..... 8  |
| 11.2    | Abstract syntax..... 8   |
| 11.3    | Negotiation of security audit trail reporting functional unit ..... 9                    |
| 12      | Relationships with other functions ..... 10  |
| 13      | Conformance ..... 10   |
| 13.1    | General conformance class requirements..... 10   |
| 13.2    | Dependent conformance class requirements ..... 10  |
| 13.3    | Management information conformance requirements ..... 11                                 |
| 13.4    | PICS requirements ..... 11   |
| Annex A | Definition of management information..... 12   |
| Annex B | MCS proforma ..... 14  |
| Annex C | MOCS proforma ..... 16   |
| Annex D | MIDS (notification) proforma..... 19   |
| Annex E | PICS proforma ..... 20   |
| Annex F | Relationship with the security audit framework ..... 26                                  |

## INFORMATION NOTE

The following table gives a list of X.700 series Recommendations which were, developed in collaboration with the ISO/IEC and are identical to the corresponding International Standard. Cross-references to the corresponding ISO/IEC International Standard number and the short title of the Recommendation | International Standard are provided.

| CCITT Recommendation<br>ISO/IEC International Standard  | Short title  |
|---|--|
| X.700   7498-4 (Note)   | Management Framework                                 |
| X.701   10040   | Systems Management Overview                          |
| X.710   9595 (Note)   | Common Management Information Service Definition     |
| X.711   9596-1 (Note)   | Common Management Information Protocol Specification |
| X.712   9596-2  | CMIP PICS  |
| X.720   10165-1   | Management Information Model                         |
| X.721   10165-2   | Definition of Management Information                 |
| X.722   10165-4   | Guidelines for the Definition of Managed Objects     |
| X.730   10164-1   | Object Management Function                           |
| X.731   10164-2   | State Management Function                            |
| X.732   10164-3   | Attributes for Representing Relationships            |
| X.733   10164-4   | Alarm Reporting Function                             |
| X.734   10164-5   | Event report Management Function                     |
| X.735   10164-6   | Log Control Function                                 |
| X.736   10164-7   | Security Alarm Reporting Function                    |
| X.740   10164-8   | Security Audit Trail Function                        |
| NOTE – This Recommendation and International Standard are not identical, but are technically aligned. |  |

## INTERNATIONAL STANDARD

## CCITT RECOMMENDATION

**INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION –  
SYSTEMS MANAGEMENT: SECURITY AUDIT TRAIL FUNCTION**

**1 Scope**

This Recommendation | International Standard defines the security audit trail function. The security audit trail function is a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information and commands for the purpose of systems management, as defined by CCITT Rec. X.700 | ISO 7498-4. This Recommendation | International Standard is positioned in the application layer of CCITT Rec. X.200 | ISO 7498 and is defined according to the model provided by ISO/IEC 9545. The role of systems management functions is described by CCITT Rec. X.701 | ISO/IEC 10040.

This Recommendation | International Standard

- establishes user requirements for the service definition needed to support the security audit trail reporting function;
- defines the service provided by the security audit trail reporting function;
- specifies the protocol that is necessary in order to provide the service;
- defines the relationship between the service and management notifications;
- defines relationships with other systems management functions;
- specifies conformance requirements.

This Recommendation | International Standard does not define

- a security audit, nor how to perform one. A security audit may be used to assist in assessing the effectiveness of a security policy. The security policy identifies the categories of security-related events that require auditing, and the location of the security audit trail log in which they are to be recorded;
- the nature of any implementation intended to provide the security audit trail function;
- the occasions where the use of the security audit trail function is appropriate;
- the services necessary for the establishment, normal and abnormal release of a management association;
- any other notifications defined by other Recommendations | International Standards which may be of interest to a security administrator.

**2 Normative references**

The following CCITT Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent editions of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The CCITT Secretariat maintains a list of currently valid CCITT Recommendations.

## 2.1 Identical Recommendations | International Standards

- CCITT Recommendation X.701 (1992) | ISO/IEC 10040:1992, *Information technology – Open Systems Interconnection – Systems management overview.*
- CCITT Recommendation X.721 (1992) | ISO/IEC 10165-2:1992, *Information technology – Open Systems Interconnection – Structure of management information: Definition of management information.*
- CCITT Recommendation X.722 (1992) | ISO/IEC 10165-4:1992, *Information technology – Open Systems Interconnection – Structure of management information: Guidelines for the definition of managed objects.*
- CCITT Recommendation X.724<sup>1)</sup> | ISO/IEC 10165-6<sup>1)</sup>, *Information technology – Open Systems Interconnection – Structure of management information: Requirements and guidelines for implementation conformance statement proformas associated with management information.*
- CCITT Recommendation X.733 (1992) | ISO/IEC 10164-4:1992, *Information technology – Open Systems Interconnection – Systems management: Alarm reporting function.*
- CCITT Recommendation X.734 (1992) | ISO/IEC 10164-5:1993, *Information technology – Open Systems Interconnection – Systems management: Event report management function.*
- CCITT Recommendation X.735 (1992) | ISO/IEC 10164-6:1993, *Information technology – Open Systems Interconnection – Systems management: Log control function.*
- CCITT Recommendation X.736 (1992) | ISO/IEC 10164-7:1992, *Information technology – Open Systems Interconnection – Systems management: Security alarm reporting function.*

## 2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.200 (1988), *Reference Model of Open Systems Interconnection for CCITT applications.*  
ISO 7498:1984, *Information processing systems – Open Systems Interconnection – Basic Reference Model.*
- CCITT Recommendation X.208 (1988), *Specification of Abstract Syntax Notation One (ASN.1).*  
ISO/IEC 8824:1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1).*
- CCITT Recommendation X.209 (1988), *Specification of basic encoding rules for Abstract Syntax Notation (ASN.1).*  
ISO/IEC 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*
- CCITT Recommendation X.210 (1988), *Open Systems Interconnection layer service definition conventions.*  
ISO/TR 8509:1987, *Information processing systems – Open Systems Interconnection – Service conventions.*
- CCITT Recommendation X.290 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications – General concepts.*  
ISO/IEC 9646-1:1991, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 1: General concepts.*
- CCITT Recommendation X.291 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications – Abstract test suite specification.*  
ISO/IEC 9646-2 : 1991, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 2: Abstract test suite specification.*
- CCITT Recommendation X.700 (1992), *Management framework definition for Open Systems Interconnection for CCITT applications.*  
ISO/IEC 7498-4:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework.*
- CCITT Recommendation X.710 (1991), *Common management information service definition for CCITT applications.*

---

<sup>1)</sup> Presently at the stage of draft.

ISO/IEC 9595:1991, *Information technology – Open Systems Interconnection – Common management information service definition.*

- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security architecture.*

### 2.3 Additional references

- ISO/IEC 9545:1989, *Information technology – Open Systems Interconnection – Application Layer structure.*
- ISO/IEC 10181-7<sup>1)</sup>, *Information technology – Open Systems Interconnection – Security frameworks – Part 7: Security audit framework.*

## 3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

### 3.1 Basic reference model definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.200 | ISO 7498:

open system.

### 3.2 Security architecture definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.800 | ISO 7498-2:

- a) security audit trail;
- b) security policy.

### 3.3 Management framework definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.700 | ISO 7498-4:

managed object.

### 3.4 Systems management overview definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.701 | ISO/IEC 10040:

- a) agent role;
- b) dependent conformance;
- c) general conformance;
- d) management domain;
- e) manager role;
- f) notification;
- g) systems management functional unit.

<sup>1)</sup> Presently at the stage of draft.

### 3.5 Event report management definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.734 | ISO/IEC 10164-5:

discriminator.

### 3.6 Security alarm reporting definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.736 | ISO/IEC 10164-7:

security-related event.

### 3.7 Log control definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.735 | ISO/IEC 10164-6:

- a) log;
- b) log record.

### 3.8 OSI conformance testing definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.290 | ISO/IEC 9646-1:

- a) PICS proforma;
- b) protocol implementation conformance statement (PICS);
- c) system conformance statement.

## 4 Abbreviations

|       |   |
|-------|---|
| ASN.1 | Abstract Syntax Notation One                    |
| CMIS  | Common Management Information Services          |
| Conf  | Confirmation                                    |
| Ind   | Indication                                      |
| MAPDU | Management Application Protocol Data Unit       |
| MCS   | Management conformance summary                  |
| MIDS  | Management information definition statement     |
| MOCS  | Managed object conformance statement            |
| OSI   | Open Systems Interconnection                    |
| PICS  | Protocol implementation conformance statement   |
| Req   | Request   |
| Rsp   | Response  |
| SMAPM | Systems Management Application Protocol Machine |

## 5 Conventions

This Recommendation | International Standard defines services for the security audit trail function using the descriptive conventions defined in CCITT Rec. X.210 | ISO/TR 8509. In clause 9, the definition of each service includes a table that lists the parameters of its primitives. For a given primitive, the presence of each parameter is described by one of the following values:

- M the parameter is mandatory;
- (=) the value of the parameter is equal to the value of the parameter in the column to the left;
- U the use of the parameter is a service-user option;



- the parameter is not present in the interaction described by the primitive concerned;
- C the parameter is conditional. The condition(s) are defined by the text which describes the parameter;
- P subject to the constraints imposed on the parameter by CCITT Rec. X.710 | ISO/IEC 9595.

NOTE – The parameters that are marked “P” in Table 1 are mapped directly onto the corresponding parameters of the CMIS service primitive, without changing the semantics or syntax of the parameters. The remaining parameters are used to construct an MAPDU.

## 6 Requirements

The security management user requires the ability to record in a security audit trail log, security-related events that occur in the management domain. The security policy of an open system may require that particular security-related events be sent to a security audit trail log in the same or in a different open system.

The types of security-related event that may be subject to security auditing include, but are not limited to

- connections;
- disconnections;
- security mechanism utilization;
- management operations; and
- usage accounting.

The security management user also requires the ability to control the operation of the security audit trail function.

This Recommendation | International Standard describes the use of services and techniques to satisfy these requirements.

## 7 Model

This Recommendation | International Standard requires that the security-related events shall be logged according to the procedures defined in CCITT Rec. X.735 | ISO/IEC 10164-6. The discriminator construct within the security audit trail log shall be specified so as to permit the capture of incoming events that the security policy requires to be logged. If the event reports are to be sent to a different destination, then event forwarding discriminators as defined in CCITT Rec. X.734 | ISO/IEC 10164-5 shall be created and the destination address shall be set to send the event to the system where the selected security audit trail log is located. The security audit trail log is a log as defined in CCITT Rec. X.735 | ISO/IEC 10164-6.

The model for conveying event reports to the system where the security audit trail log is situated is defined in CCITT Rec. X.734 | ISO/IEC 10164-5. The model for the creation and retrieval of entries in the security audit trail log is defined in CCITT Rec. X.735 | ISO/IEC 10164-6.

## 8 Generic definitions

### 8.1 Generic notifications

This Recommendation | International Standard defines a set of generic security audit trail notifications and their applicable parameters and semantics.

The set of generic notifications, parameters and semantics defined by this Recommendation | International Standard provide the detail for the following parameters of the M-EVENT-REPORT service as defined by CCITT Rec. X.710 | ISO/IEC 9595:

- event type;
- event information;
- event reply.

All notifications are potential entries in a systems management log. CCITT Rec. X.721 | ISO/IEC 10165-2 defines a generic event log record object class from which all entries are derived, the additional information being specified by the event information and event reply parameters.

### **8.1.1 Event type**

This parameter defines the type of the security audit trail report. The following event types are defined in this Recommendation | International Standard

- Service report: an indication of an event appertaining to the provision, denial or recovery of a service. Specific causes for the generation of the event are described in 8.1.2;
- Usage report: an indication of a record which contains information of a statistical nature, relevant to security.

Other notifications defined in other Recommendations | International Standards (for example, CCITT Rec. X.736 | ISO/IEC 10164-7) may be recorded in the security audit trail log. The notification types (analagous to security audit trail report types) and their associated parameters are defined in the appropriate Recommendations | International Standard.

### **8.1.2 Event information**

The service report cause parameter consitutes the notification specific event information.

This parameter shall be supplied when the event type specifies a service report, and defines further qualification as to the probable cause of the service report. The value of this parameter in combination with the value of event type, determines which parameters constitute the balance of the service report, and what the possible values of those parameters may be.

Service report cause values for notifications shall be indicated in the behaviour clause of the object class definition. This Recommendation | International Standard defines, for use within the systems management application context defined in CCITT Rec. X.701 | ISO/IEC 10040, service report causes that have wide applicability across managed object classes. These values are registered in Annex A of this Recommendation | International Standard. The syntax of service report causes shall be the ASN.1 type object identifier. Additional service report causes, for use within the systems management application context defined in CCITT Rec. X.701 | ISO/IEC 10040, may be added to this Recommendation | International Standard and registered using the registration procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

Other service report causes, for use within the systems management application context defined in CCITT Rec. X.701 | ISO/IEC 10040, may be defined outside of this Recommendation | International Standard and registered using the registration procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

The following service report cause values are defined

- Request for service: this value specifies that the notification has been generated because of a request for the provision of a service;
- Denial of service: this value specifies that the notification has been generated because a request for service has been denied;
- Response from service: this value specifies that the notification has been generated because a request for service has been satisfied;
- Service failure: this value specifies that the notification has been generated because an abnormal condition that caused the service to fail, has been detected during the provision of a service;
- Service recovery: this value specifies that the notification has been generated because a service has recovered from an abnormal condition;
- Other reason: this value specifies that the notification has been generated for reasons other than those listed above. The actual cause and other relevant information is specified in the other parameters of the report.

### **8.1.3 Event reply**

This Recommendation | International Standard does not specify management information to be used in the event reply parameter.

## **8.2 Managed object**

A security audit trail record is a managed object class derived from the event log record object class defined in CCITT Rec. X.721 | ISO/IEC 10165-2. The security audit trail record object class represents information stored in logs resulting from security audit trail notifications.

### 8.3 Imported generic definitions

The following parameters are also utilized. These parameters are defined by CCITT Rec. X.733 | ISO/IEC 10164-4.

- Additional information;
- Additional text;
- Correlated notifications;
- Notification identifier.

### 8.4 Compliance

Managed object class definitions support the functions defined in this Recommendation | International Standard by incorporating the specification of the notifications through reference to the notification templates defined in Annex A. The reference mechanism is defined in CCITT Rec. X.722 | ISO/IEC 10165-4.

A managed object class definition importing one or more of the security audit trail notifications defined in this Recommendation | International Standard is required for each instance of a security audit trail report to select the security audit trail report type that most closely reflects the real event that leads to the managed object issuing the notification. The definition of the managed object class shall, for each imported notification, specify in the behaviour clause which of the optional and conditional parameters are to be utilized, the conditions for their use, and their values. It is permissible to state that the use of a parameter remains optional.

## 9 Service definition

### 9.1 Introduction

Security audit trail notifications provide the ability to report security-related events detected by a managed object. The parameters convey the information relevant to the security audit trail.

### 9.2 Security audit trail reporting service

The security audit trail reporting service uses the parameters defined in clause 8 in addition to the general M EVENT-REPORT service parameters defined in CCITT Rec. X.710 | ISO/IEC 9595. Table 1 lists the parameters for the security audit trail reporting service.

**Table 1 – Security audit trail reporting parameters**

| Parameter name                            | Req/Ind | Rsp/Conf |
|---|---------|----------|
| Invoke identifier                         | P       | P        |
| Mode                                      | P       | –        |
| Managed object class                      | P       | P        |
| Managed object instance                   | P       | P        |
| Event type                                | M       | C(=)     |
| Event time                                | P       | –        |
| Event information<br>Service report cause | C       | –        |
| Notification identifier                   | U       | –        |
| Correlated notifications                  | U       | –        |
| Additional text                           | U       | –        |
| Additional information                    | U       | –        |
| Current time                              | –       | P        |
| Event reply                               | –       | –        |
| Errors                                    | –       | P        |

The Event time, Correlated notifications, and Notification identifier parameters may be assigned by the managed object that emits the notification or by the managed system.

## 10 Functional units

The security audit trail function constitutes a single systems management functional unit.

## 11 Protocol

### 11.1 Elements of procedure

#### 11.1.1 Agent role

##### 11.1.1.1 Invocation

The security audit trail reporting procedures are initiated by the security audit trail reporting request primitive. On receipt of a security audit trail reporting request primitive, the SMAPM shall construct an MAPDU and issue a CMIS M-EVENT-REPORT request service primitive with parameters derived from the security audit trail reporting request primitive. In the non-confirmed mode, the procedure in 11.1.1.2 does not apply.

##### 11.1.1.2 Receipt of response

On receipt of a CMIS M-EVENT-REPORT confirm service primitive containing an MAPDU responding to a security audit trail reporting notification, the SMAPM shall issue a security audit trail reporting confirmation primitive to the security audit trail reporting service user with parameters derived from the CMIS M-EVENT-REPORT confirm service primitive, thus completing the security audit trail reporting procedure.

NOTE – The SMAPM shall ignore all errors in the received MAPDU. The security audit trail reporting service user may ignore such errors, or abort the association as a consequence of such errors.

#### 11.1.2 Manager role

##### 11.1.2.1 Receipt of request

On receipt of a CMIS M-EVENT-REPORT indication service primitive containing an MAPDU requesting the security audit trail reporting service, the SMAPM shall, if the MAPDU is well formed, issue a security audit trail reporting indication primitive to the security audit trail reporting service user with parameters derived from the CMIS M-EVENT-REPORT indication service primitive. Otherwise, the SMAPM shall in the confirmed mode construct an appropriate MAPDU containing notification of the error, and shall issue a CMIS M-EVENT-REPORT response service primitive with an error parameter present. In the non-confirmed mode, the procedure in 11.1.2.2 does not apply.

##### 11.1.2.2 Response

In the confirmed mode, the SMAPM shall accept a security audit trail reporting response primitive and shall construct an MAPDU confirming the notification and issue a CMIS M-EVENT-REPORT response service primitive with the parameters derived from the security audit trail reporting response primitive.

## 11.2 Abstract syntax

### 11.2.1 Managed objects

This Recommendation | International Standard defines the following support object, the abstract syntax of which is specified in Annex A.

securityAuditTrailRecord.

### 11.2.2 Attributes

Table 2 identifies the relationship between the parameter defined in 8.1.2 and attribute type specification defined in Annex A.

Table 2 – Attributes

| Parameter    | Attribute name     |
|--------------|--------------------|
| report cause | serviceReportCause |

### 11.2.3 Attribute groups

There are no attribute groups defined by this systems management function.

### 11.2.4 Actions

There are no specific actions defined by this systems management function.

### 11.2.5 Notifications

Table 3 identifies the relationship between the notifications defined in 8.1.1 and the notification type specifications defined in Annex A.

**Table 3 – Notifications**

| Security audit trail type | Notification type |
|---------------------------|-------------------|
| Service report            | serviceReport     |
| Usage report              | usageReport       |

The abstract syntax referenced by the notification type specifications is carried in the MAPDU.

### 11.2.6 Service report causes

Table 4 identifies the relationship between the service report causes defined in 8.1.2 and the ASN.1 value references defined in Annex A.

**Table 4 – Service report causes**

| Service report cause  | ASN.1 value reference |
|-----------------------|-----------------------|
| Request for service   | serviceRequest        |
| Denial of service     | serviceDenial         |
| Response from service | serviceResponse       |
| Service failure       | serviceFailure        |
| Service recovery      | serviceRecovery       |
| Other reason          | otherReason           |

## 11.3 Negotiation of security audit trail reporting functional unit

This Recommendation | International Standard assigns the object identifier

**{joint-iso-ccitt ms(9) function(2) part8(8) functionalUnitPackage(1)}**

as a value of the ASN.1 type FunctionalUnitPackageId defined in CCITT Rec. X.701 | ISO/IEC 10040 to use for negotiating the following functional unit

0 security audit trail reporting functional unit

where the number identifies the bit position assigned to the functional unit, and the name references the functional unit as defined in clause 10.

Within the Systems management application context, the mechanism for negotiating the security audit trail reporting functional unit is described by CCITT Rec. X.701 | ISO/IEC 10040.

NOTE – The requirement to negotiate functional units is specified by the application context.

## 12 Relationships with other functions

Control of the security audit trail reporting service is provided by mechanisms specified in CCITT Rec. X.734 | ISO/IEC 10164-5. Modification of the security audit trail log attributes is provided by CCITT Rec. X.735 | ISO/IEC 10164-6.

The security audit trail notification service may exist independently of the control services of CCITT Rec. X.734 | ISO/IEC 10164-5 and of CCITT Rec. X.735 | ISO/IEC 10164-6.

## 13 Conformance

There are two conformance classes: general conformance class and dependent conformance class. A system claiming to implement the elements of procedure for the security audit trail reporting functional unit defined in this Recommendation | International Standard shall comply with the requirements for either the general or the dependent conformance class as defined in the following clauses. The supplier of the implementation shall state the class to which conformance is claimed.

NOTE – The use of the two terms “general conformance class” and “dependent conformance class”, is under review. However, this standard continues to use these terms in order to be consistent with CCITT Rec. X.740 | ISO/IEC 10040 and other standards under the general title *Information technology – Open Systems Interconnection – Systems management*. When the review has been completed, it is intended to clarify and/or correct this conformance clause together with the related clauses in those other Recommendations | International Standards.

### 13.1 General conformance class requirements

A system claiming general conformance to this Recommendation | International Standard shall support this systems management function for all managed object classes that import management information defined by this Recommendation | International Standard.

#### 13.1.1 Static conformance

The system shall

- a) support the role of manager or agent or both, with respect to the security audit trail reporting functional unit;
- b) support the transfer syntax derived from the encoding rules specified in CCITT Rec. X.209 | ISO/IEC 8825 and named

**{joint-iso-ccitt asn1(1) basic encoding(1)}**

for the purpose of generating and interpreting the MAPDUs, defined by the abstract data types referenced in 11.2.5.

#### 13.1.2 Dynamic conformance

The system shall support the elements of procedure defined in this Recommendation | International Standard for the security audit trail reporting service in the role(s) for which conformance is claimed.

### 13.2 Dependent conformance class requirements

#### 13.2.1 Static conformance

The system shall support the transfer syntax derived from the encoding rules specified in CCITT Rec. X.209 | ISO/IEC 8825 and named

**{joint-iso-ccitt asn1(1) basic encoding(1)}**

for the purpose of generating and interpreting the MAPDUs, defined by the abstract data types referenced in 11.2.5 of this Recommendation | International Standard, as required by a referencing specification.

#### 13.2.2 Dynamic conformance

The system shall support the elements of procedure defined in this Recommendation | International Standard as required by a referencing specification.

### 13.3 Management information conformance requirements

A MCS proforma which conforms to this Recommendation | International Standard shall be textually identical to the MCS proforma specified in Annex B, differing only in pagination and page headers. A security audit trail report record object class MOCS proforma which conforms to this Recommendation | International Standard shall be textually identical to the MOCS proforma specified in Annex C, differing only in pagination and page headers. A security audit trail notification MIDS proforma which conforms to this Recommendation | International Standard shall be textually identical to the MIDS proforma specified in Annex D, differing only in pagination and page headers. A system which conforms to this Recommendation | International Standard shall

- describe an implementation which conforms to this Recommendation | International Standard;
- be a conforming MCS, MOCS or MIDS proforma which has been completed in accordance with the instructions for completion given in CCITT Rec. X.724 | ISO/IEC 10165-6;
- include the information necessary to uniquely identify both the supplier and the implementation.

The supplier of an implementation which is claimed to conform to this Recommendation | International Standard shall complete a copy of the management conformance summary provided in Annex B as part of the conformance requirements, and shall provide the information necessary to identify both the supplier and the implementation.

### 13.4 PICS requirements

A PICS proforma which conforms to this Recommendation | International Standard shall be textually identical to Annex E, differing only in pagination and page headers. A PICS which conforms to this Recommendation | International Standard shall

- describe an implementation which conforms to this Recommendation | International Standard;
- be a conforming PICS proforma which has been completed in accordance with the instructions for completion given in E.1;
- include the information necessary to uniquely identify both the supplier and the implementation.

The supplier of a protocol implementation which is claimed to conform to this Recommendation | International Standard shall complete a copy of the PICS proforma provided in Annex E as part of the conformance requirements, and shall provide the information necessary to identify both the supplier and the implementation.

## Annex A

### Definition of management information

(This annex forms an integral part of this Recommendation | International Standard)

#### A.1 Allocation of object identifiers

This Recommendation | International Standard allocates the following object identifiers

**SecurityAuditTrailDefinitions** {joint-iso-ccitt ms(9) function(2) part8(8) asn1Module(2) 1}

**DEFINITIONS ::= BEGIN**

**securityAuditTrail-Object OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) managedObjectClass(3)}**

**securityAuditTrail-Package OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) package(4)}**

**securityAuditTrail-Attribute OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) attribute(7)}**

**securityAuditTrail-Notification OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) notification(10)}**

**serviceReportCause OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) standardSpecificExtension(0) 1}**

-- the following OBJECT IDENTIFIER values can be used as values for the service report cause parameter in A.5.

**serviceRequest ServiceReportCause ::= {serviceReportCause 1}**

**serviceDenial ServiceReportCause ::= {serviceReportCause 2}**

**serviceResponse ServiceReportCause ::= {serviceReportCause 3}**

**serviceFailure ServiceReportCause ::= {serviceReportCause 4}**

**serviceRecovery ServiceReportCause ::= {serviceReportCause 5}**

**otherReason ServiceReportCause ::= {serviceReportCause 6}**

**END**

#### A.2 Definition of managed object classes

The securityAuditTrailRecord object class is used to define the information stored in a log as the result of security audit trail notifications or event reports.

**securityAuditTrailRecord** MANAGED OBJECT CLASS

DERIVED FROM "CCITT Rec. X.721 | ISO/IEC 10165-2 : 1992":eventLogRecord;

CONDITIONAL PACKAGES

**serviceReportCausePackage** PACKAGE

    BEHAVIOUR

**serviceReportCausePackageBehaviour** BEHAVIOUR

            DEFINED AS "This package provides further qualification as to the probable cause of a service report.";

    ;

**ATTRIBUTES** serviceReportCause GET;

**REGISTERED AS** {securityAuditTrail-Package 1};

**PRESENT IF** "This package shall be present if the notification concerns a service report.";

**REGISTERED AS** {securityAuditTrail-Object 1};

#### A.3 Definition of attributes

**serviceReportCause** ATTRIBUTE

**WITH ATTRIBUTE SYNTAX** SecurityAuditTrail-ASN1Module.ServiceReportCause;

**MATCHES FOR EQUALITY**;

    BEHAVIOUR

**serviceReportCauseBehaviour** BEHAVIOUR

            DEFINED AS "This attribute is used to provide the reason for the service report. The value of this attribute is an OBJECT IDENTIFIER that has been registered by a registration authority. Some of the possible values of this attribute are specified by, and registered in this Recommendation | International Standard.";

    ;

**REGISTERED AS** {securityAuditTrail-Attribute 1};



**A.4 Definition of notification types****A.4.1 Service Report**

serviceReport NOTIFICATION

BEHAVIOUR serviceReportBehaviour;

WITH INFORMATION SYNTAX SecurityAuditTrail-ASN1Module.SecurityAuditInfo

AND ATTRIBUTE IDS

serviceReportCause serviceReportCause,  
 notificationIdentifier notificationIdentifier,  
 correlatedNotifications correlatedNotifications,  
 additionalText additionalText,  
 additionalInformation additionalInformation;

REGISTERED AS {securityAuditTrail-Notification 1};

serviceReportBehaviour BEHAVIOUR

DEFINED AS "This notification type is used to report information about a service request, denial, response, recovery or other information which is relevant to the security administrator.";

**A.4.2 Usage Report**

usageReport NOTIFICATION

BEHAVIOUR usageReportBehaviour;

WITH INFORMATION SYNTAX SecurityAuditTrail-ASN1Module.SecurityAuditInfo

AND ATTRIBUTE IDS

notificationIdentifier notificationIdentifier,  
 correlatedNotifications correlatedNotifications,  
 additionalText additionalText,  
 additionalInformation additionalInformation;

REGISTERED AS {securityAuditTrail-Notification 2};

usageReportBehaviour BEHAVIOUR

DEFINED AS "This notification type is used to report information of a statistical nature which is relevant to the security administrator.";

**A.5 Abstract syntax definitions**

SecurityAuditTrail-ASN1Module {joint-iso-ccitt ms(9) function(2) part8(8) asn1Module(2) 2}

DEFINITIONS ::= BEGIN

IMPORTS

AdditionalText, AdditionalInformation, CorrelatedNotifications, NotificationIdentifier

FROM Attribute-ASN1Module {joint-iso-ccitt ms(9) smi(3) part2(2) asn1Module(2) 1}

SecurityAuditInfo ::= SEQUENCE {  
     serviceReportCause       IMPLICIT ServiceReportCause OPTIONAL,  
     notificationIdentifier   IMPLICIT NotificationIdentifier OPTIONAL,  
     correlatedNotifications [1] IMPLICIT CorrelatedNotifications OPTIONAL,  
     additionalText           IMPLICIT AdditionalText OPTIONAL,  
     additionalInformation   [2] IMPLICIT AdditionalInformation OPTIONAL }

ServiceReportCause ::= OBJECT IDENTIFIER

END

## Annex B MCS proforma<sup>2)</sup>

(This annex forms an integral part of this Recommendation | International Standard)

### B.1 Introduction

#### B.1.1 Symbols, abbreviations and terms

The following abbreviations are used throughout the proformas:

- o.N (N is an INTEGER) support of at least one of the choices is required
- dmi-att **joint-iso-ccitt ms(9) smi(3) part2(2) attribute(7)**
- dmi-nb **joint-iso-ccitt ms(9) smi(3) part2(2) nameBinding(6)**
- dmi-pkg **joint-iso-ccitt ms(9) smi(3) part2(2) package(4)**
- satf-att **joint-iso-ccitt ms(9) function(2) part8(8) attribute(7)**
- satf-not **joint-iso-ccitt ms(9) function(2) part8(8) notification(10)**

#### B.1.2 Table format

Some of the tables in Annexes C and D have been split because the information is too wide to fit on the page. Where this occurs, the index number of the first block of columns has a lower case “a” appended, and index number of the second block of columns has a lower case “b” appended. A complete table reconstructed from the constituent parts should have the following layout.

|       |                             |                             |
|-------|-----------------------------|-----------------------------|
| Index | Columns associated with “a” | Columns associated with “b” |
|-------|-----------------------------|-----------------------------|

### B.2 Identification of the implementation

#### B.2.1 Date of statement

The supplier of the implementation shall enter the date of this statement in the box below. Use the format DD-MM-YYYY.

|                   |
|-------------------|
| Date of statement |
|-------------------|

#### B.2.2 Identification of the implementation

The supplier of the implementation shall enter information necessary to uniquely identify the implementation and the system(s) in which it may reside, in the box below.

|  |
|--|
|  |
|--|

<sup>2)</sup> Users of this Recommendation | International Standard may freely reproduce the MCS proforma in this annex so that it can be used for its intended purpose, and may further publish the completed MCS. Instructions for completing the MCS proforma are specified in CCITT Rec. X.724 | ISO/IEC 10165-6.

**B.2.3 Contact**

The supplier of the implementation shall provide information on whom to contact if there are any queries concerning the content of the MCS, in the box below.

**B.3 Identification of the Recommendation | International Standard in which the management information is defined**

The supplier of the implementation shall enter the title, reference number and date of the publication of the Recommendation | International Standard which specifies the management information to which conformance is claimed, in the box below.

Recommendation | International Standard to which conformance is claimed

**B.3.1 Technical corrigenda implemented**

The supplier of the implementation shall enter the reference numbers of implemented technical corrigenda which modify the identified Recommendation | International Standard, in the box below.

**B.3.2 Amendments implemented**

The supplier of the implementation shall state the titles and reference numbers of implemented amendments to the identified Recommendation | International Standard, in the box below.

**B.4 Management conformance summary**

The supplier of the implementation shall provide information on whether the implementation claims conformance to any of the set of Recommendations | International Standards globally representing the implementation under claim. For each Recommendation | International Standard the supplier of the implementation claims conformance to, the corresponding conformance statement(s) shall be completed, or referenced, by the MCS. The supplier of the implementation shall complete the Support and Additional information columns.

| Identification of the Recommendation   International Standard that includes the proforma | Reference of MOCS proforma | Managed object class template label | Status | Support | Additional information |
|--|----------------------------|-------------------------------------|--------|---------|------------------------|
| CCITT Rec. X.740   ISO/IEC 10164-8   | Annex C                    | securityAuditTrailRecord            | m      |         |                        |

**Annex C**  
**MOCS proforma<sup>3)</sup>**

(This annex forms an integral part of this Recommendation | International Standard)

**C.1 Statement of conformance to the managed object class**

|                                     |  |
|-------------------------------------|--|
| Managed object class template label | Value of OBJECT IDENTIFIER for the class                             |
| securityAuditTrailRecord            | {joint-iso-ccitt ms(9) function(2) part8(8) managedObjectClass(3) 1} |

The supplier of the implementation shall state whether or not all mandatory features of the security audit trail record are supported, in Table C.1.

**Table C.1 – Feature support**

| Index |   | Support |
|-------|---|---------|
| C.1.1 | Are all mandatory features of the managed object class supported? |         |
| C.1.2 | Do instances of the managed object class support allomorhism?     |         |

**C.2 Name bindings**

The supplier of the implementation shall state which name bindings in which instances of the managed object class can be subordinate are supported, in the Support and Additional information columns of Table C.2.

**Table C.2 – Name binding support**

| Index  | Name binding template label | Value of OBJECT IDENTIFIER for name binding | Superior object class template label                           | Status | Support |
|--------|-----------------------------|---|--|--------|---------|
| C.2.1a | logRecord-log               | {dmi-nb 3}                                  | “CCITT Rec. X.721   ISO/IEC 10165-2 : 1992”:log AND SUBCLASSES | o      |         |

**Table C.2 (concluded) – Name binding support**

| Index  | Status          |                 | Support         |                 | Additional information |
|--------|-----------------|-----------------|-----------------|-----------------|------------------------|
|        | Object creation | Object deletion | Object creation | Object deletion |                        |
| C.2.1b | x               | m               |                 |                 |                        |

<sup>3)</sup> Users of this Recommendation | International Standard may freely reproduce the MOCS proforma in this annex so that it can be used for its intended purpose, and may further publish the completed MOCS. Instructions for completing the MOCS proforma are specified in CCITT Rec. X.724 | ISO/IEC 10165-6.

**C.3 Packages**

The supplier of the implementation shall state whether or not the packages specified by this managed object of this class are supported, in Table C.3.

**Table C.3 – Package support**

| Index | Package label                  | Value of OBJECT IDENTIFIER | Status | Support |
|-------|--------------------------------|----------------------------|--------|---------|
| C.3.1 | eventTimePackage               | {dmi-pkg 11}               | o      |         |
| C.3.2 | notificationIdentifierPackage  | {dmi-pkg 24}               | o      |         |
| C.3.3 | correlatedNotificationsPackage | {dmi-pkg 23}               | o      |         |
| C.3.4 | additionalTextPackage          | {dmi-pkg 19}               | o      |         |
| C.3.5 | additionalInformationPackage   | {dmi-pkg 18}               | o      |         |

**C.4 Attributes**

The supplier of the implementation shall state whether or not the attributes specified by all of the packages instantiated in a managed object of this class are supported, in the Support and Additional information columns of Table C.4. The supplier of the implementation shall indicate support for each of the operations for each attribute supported.

**Table C.4 — Attribute support**

| Index   | Attribute template label | Value of OBJECT IDENTIFIER | Status      |     |         |     |        |              |
|---------|--------------------------|----------------------------|-------------|-----|---------|-----|--------|--------------|
|         |                          |                            | SetByCreate | Get | Replace | Add | Remove | SetToDefault |
| C.4.1a  | objectClass              | {dmi-att 65}               | x           | m   | x       | x   | x      | x            |
| C.4.2a  | nameBinding              | {dmi-att 63}               | x           | m   | x       | x   | x      | x            |
| C.4.3a  | packages                 | {dmi-att 66}               | x           | c1  | x       | x   | x      | x            |
| C.4.4a  | allomorphs               | {dmi-att 50}               | x           | c2  | x       | x   | x      | x            |
| C.4.5a  | logRecordId              | {dmi-att 3}                | x           | m   | x       | x   | x      | x            |
| C.4.6a  | loggingTime              | {dmi-att 59}               | x           | m   | x       | x   | x      | x            |
| C.4.7a  | managedObjectClass       | {dmi-att 60}               | x           | m   | x       | x   | x      | x            |
| C.4.8a  | managedObjectInstance    | {dmi-att 61}               | x           | m   | x       | x   | x      | x            |
| C.4.9a  | eventType                | {dmi-att 14}               | x           | m   | x       | x   | x      | x            |
| C.4.10a | eventTime                | {dmi-att 13}               | x           | c3  | x       | x   | x      | x            |
| C.4.11a | notificationIdentifier   | {dmi-att 16}               | x           | c4  | x       | x   | x      | x            |
| C.4.12a | correlatedNotifications  | {dmi-att 12}               | x           | c5  | x       | x   | x      | x            |
| C.4.13a | additionalText           | {dmi-att 7}                | x           | c6  | x       | x   | x      | x            |
| C.4.14a | additionalInformation    | {dmi-att 6}                | x           | c7  | x       | x   | x      | x            |
| C.4.15a | serviceReportCause       | {sarf-att 1}               | x           | m   | x       | x   | x      | x            |

- c1: if C.3.1 or C.3.2 or C.3.3 or C.3.4 or C.3.5 then m else —
- c2: if C.1.2 then m else —
- c3: if C.3.1 then m else —
- c4: if C.3.2 then m else —
- c5: if C.3.3 then m else —
- c6: if C.3.4 then m else —
- c7: if C.3.5 then m else —

Table C.4 (concluded) — Attribute support

| Index   | Support     |     |         |     |        |              | Additional information |
|---------|-------------|-----|---------|-----|--------|--------------|------------------------|
|         | SetByCreate | Get | Replace | Add | Remove | SetToDefault |                        |
| C.4.1b  |             |     |         |     |        |              |                        |
| C.4.2b  |             |     |         |     |        |              |                        |
| C.4.3b  |             |     |         |     |        |              |                        |
| C.4.4b  |             |     |         |     |        |              |                        |
| C.4.5b  |             |     |         |     |        |              |                        |
| C.4.6b  |             |     |         |     |        |              |                        |
| C.4.7b  |             |     |         |     |        |              |                        |
| C.4.8b  |             |     |         |     |        |              |                        |
| C.4.9b  |             |     |         |     |        |              |                        |
| C.4.10b |             |     |         |     |        |              |                        |
| C.4.11b |             |     |         |     |        |              |                        |
| C.4.12b |             |     |         |     |        |              |                        |
| C.4.13b |             |     |         |     |        |              |                        |
| C.4.14b |             |     |         |     |        |              |                        |
| C.4.15b |             |     |         |     |        |              |                        |

**C.5 Attribute groups**

There are no attribute groups specified for this managed object class.

**C.6 Actions**

There are no actions specified for this managed object class.

**C.7 Notifications**

There are no notifications specified for this managed object class.

**C.8 Parameters**

There are no parameters specified for this managed object class.

## Annex D

### MIDS (notification) proforma<sup>4)</sup>

(This annex forms an integral part of this Recommendation | International Standard)

The specifier of a managed object class that claims to support the notifications specified by CCITT Rec. X.740 | ISO/IEC 10164-8 shall import a copy of this annex and complete it according to the instructions specified in CCITT Rec. X.724 | ISO/IEC 10165-6.

**Table D.1 – Notification support**

| Index    | Notification template label | Value of OBJECT IDENTIFIER | Status | Support   |               | Additional information |
|----------|-----------------------------|----------------------------|--------|-----------|---------------|------------------------|
|          |                             |                            |        | Confirmed | Non-confirmed |                        |
| D.1.1a   | serviceReport               | <b>{sarf-not 1}</b>        |        |           |               |                        |
| D.1.1.1a | –                           | –                          | –      | –         | –             | –                      |
| D.1.1.2a | –                           | –                          | –      | –         | –             | –                      |
| D.1.1.3a | –                           | –                          | –      | –         | –             | –                      |
| D.1.1.4a | –                           | –                          | –      | –         | –             | –                      |
| D.1.1.5a | –                           | –                          | –      | –         | –             | –                      |
| D.1.2a   | usageReport                 | <b>{sarf-not 2}</b>        |        |           |               |                        |
| D.1.2.1a | –                           | –                          | –      | –         | –             | –                      |
| D.1.2.2a | –                           | –                          | –      | –         | –             | –                      |
| D.1.2.3a | –                           | –                          | –      | –         | –             | –                      |
| D.1.2.4a | –                           | –                          | –      | –         | –             | –                      |
| D.1.2.5a | –                           | –                          | –      | –         | –             | –                      |

**Table D.1 (concluded) – Notification support**

| Index    | Notification field name label | OBJECT IDENTIFIER value of attribute type associated with the field | Status | Support | Additional information |
|----------|-------------------------------|---|--------|---------|------------------------|
| D.1.1b   | –                             | –   | –      | –       | –                      |
| D.1.1.1b | ServiceReportCause            | <b>{sarf-att 1}</b>   | m      |         |                        |
| D.1.1.2b | NotificationIdentifier        | <b>{dmi-att 16}</b>   | o      |         |                        |
| D.1.1.3b | CorrelatedNotifications       | <b>{dmi-att 12}</b>   | o      |         |                        |
| D.1.1.4b | AdditionalText                | <b>{dmi-att 7}</b>  | o      |         |                        |
| D.1.1.5b | AdditionalInformation         | <b>{dmi-att 6}</b>  | o      |         |                        |
| D.1.2b   | –                             | –   | –      | –       | –                      |
| D.1.2.2a | ServiceReportCause            | <b>{sarf-att 1}</b>   | –      | –       | –                      |
| D.1.2.2b | NotificationIdentifier        | <b>{dmi-att 16}</b>   | o      |         |                        |
| D.1.2.3b | CorrelatedNotifications       | <b>{dmi-att 12}</b>   | o      |         |                        |
| D.1.2.4b | AdditionalText                | <b>{dmi-att 7}</b>  | o      |         |                        |
| D.1.2.5b | AdditionalInformation         | <b>{dmi-att 6}</b>  | o      |         |                        |

<sup>4)</sup> Users of this Recommendation | International Standard may freely reproduce the MIDS proforma in this annex so that it can be used for its intended purpose. Instructions for completing the MOCS proforma are specified in CCITT Rec. X.724 | ISO/IEC 10165-6.

## Annex E PICS proforma<sup>5)</sup>

(This annex forms an integral part of this Recommendation | International Standard)

### E.1 Instructions for completing the PICS proforma

#### E.1.1 Purpose and structure

The purpose of this PICS proforma is to provide a mechanism whereby a supplier of an implementation of CCITT Rec. X.740 | ISO/IEC 10164-8 may provide information in a standard form. The PICS proforma is subdivided into clauses for the following categories of information:

- implementation details;
- protocol details;
- overall conformance claim;
- implementation capabilities.

#### E.1.2 Symbols, abbreviations and terms

The PICS proforma contained in this annex is comprised of information in a tabular form in accordance with the guidelines presented in CCITT Rec. X.291 | ISO/IEC 9646-2. The following abbreviations are used:

|     |                                |
|-----|--------------------------------|
| Spt | Support                        |
| Sts | Status                         |
| TVR | Type(s), value(s) and range(s) |

The following common notations, defined in CCITT Rec. X.291 | ISO/IEC 9646-2, are used for the status (Sts) column:

|     |  |
|-----|--|
| m   | mandatory  |
| o   | optional   |
| o.N | (N is an integer) support of at least one of the choices is required |
| x   | prohibited   |
| –   | not applicable   |

The following requirements are commonly used throughout the PICS proforma:

|    |                                 |
|----|---------------------------------|
| c1 | if E.5.1 then m else –          |
| c2 | if E.5.2 or E.5.3 then m else – |

The following common notations, defined in CCITT Rec. X.291 | ISO/IEC 9646-2, are used for the support (Spt) column:

|   |                 |
|---|-----------------|
| N | not implemented |
| Y | implemented     |
| – | not applicable  |

Within this PICS proforma, space has been provided for the supplier of the implementation to specify types, values and ranges of all parameters supported. It is recommended that references to additional specifications are included where appropriate (for example, to list the OBJECT IDENTIFIER values and/or ranges supported), and that these additional specifications be appended to the completed PICS proforma.

#### E.1.3 Scoping rules

In the Status column of the tables in this Recommendation | International Standard, a mandatory element contained within an optional or conditional constructor parameter is mandatory only if the option or condition is taken.

---

<sup>5)</sup> Users of this Recommendation | International Standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose, and may further publish the completed PICS.



**E.1.4 Instructions for completing the PICS**

The supplier of the implementation shall enter an explicit statement in each of the boxes provided using the notation described in E.1.2. Specific instruction is provided in the text which precedes each table.

**E.2 Identification of the implementation****E.2.1 Date of statement**

The supplier of the implementation shall enter the date of this statement in the box below. Use the format DD-MM-YYYY.

|                   |
|-------------------|
| Date of statement |
|-------------------|

**E.2.2 Identification of the implementation**

The supplier of the implementation shall enter information necessary to uniquely identify the implementation and the system(s) in which it may reside, in the box below.

|  |
|--|
|  |
|--|

**E.2.3 Contact**

The supplier of the implementation shall provide information on whom to contact if there are any queries concerning the content of the PICS, in the box below.

|  |
|--|
|  |
|--|

**E.2.4 Relationship with the system conformance statement**

The supplier of the implementation shall provide information which describes the relationship between the PICS and the system conformance statement for the system, in the box below.

|  |
|--|
|  |
|--|

**E.3 Identification of the protocol**

The supplier of the implementation shall enter the title, reference number and date of the publication of the Recommendation | International Standard to which conformance is claimed, in the box below.

|   |
|---|
| Recommendation   International Standard to which conformance is claimed |
|---|

**E.3.1 Defect reports implemented**

The supplier of the implementation shall enter the reference numbers of implemented defect reports which modify the specification to CCITT Rec. X.740 | ISO/IEC 10164-8, in the box below.

|  |
|--|
|  |
|--|

**E.3.2 Amendments implemented**

The supplier of the implementation shall state the titles and reference numbers of implemented amendments to CCITT Rec. X.740 | ISO/IEC 10164-8, in the box below.

|  |
|--|
|  |
|--|

**E.4 Global statement of conformance**

The supplier of the implementation shall state whether or not all mandatory capabilities are implemented for CCITT Rec. X.740 | ISO/IEC 10164-8, in Table E.1.

**Table E.1 – Capabilities**

| Index |   | Support |
|-------|---|---------|
| E.1.1 | Are all mandatory capabilities implemented? |         |

NOTE – Answering NO to this question indicates non-conformance to the protocol standard. Non-supported mandatory capabilities are listed in the PICS below, explaining why the status of the implementation is abnormal.

| Capability not implemented | Reason |
|----------------------------|--------|
|                            |        |
|                            |        |
|                            |        |
|                            |        |

**E.5 Capabilities**

**E.5.1 Systems management functional unit support**

The supplier of the implementation shall state the capability for supporting the security audit trail reporting functional unit, in Table E.2.

**Table E.2 – SMFU support**

| Index | Functional unit name                           | Status | MAPDU support                | CMIS support   | Support |
|-------|--|--------|------------------------------|----------------|---------|
| E.2.1 | Security audit trail reporting functional unit | m      | serviceReport<br>usageReport | M-EVENT-REPORT |         |

**E.5.2 Systems management functional unit negotiation support**

The supplier of the implementation shall state the capability for negotiating the use of the security audit trail reporting functional unit, in Table E.3.

**Table E.3 – SMFU negotiation support**

| Index | Negotiation capability   | Status | Support |
|-------|--|--------|---------|
| E.3.1 | Does the implementation support the negotiation of the systems management functional unit? | o      |         |

**E.5.3 Management roles**

The supplier of the implementation shall state the management role for which conformance is claimed, in Table E.4.

**Table E.4 – Management role support**

| Index | Functional unit name                           | Status  |       | Support |       |
|-------|--|---------|-------|---------|-------|
|       |  | Manager | Agent | Manager | Agent |
| E.4.1 | Security audit trail reporting functional unit | o.1     | o.1   |         |       |

**E.5.4 Parameter support**

The supplier of the implementation shall state support for sending the identified parameters, in Table E.5.

**Table E.5 – Parameter support**

| Index | Parameter name          | Status | Support |
|-------|-------------------------|--------|---------|
| E.5.1 | CorrelatedNotifications | o      |         |
| E.5.2 | AdditionalText          | o      |         |
| E.5.3 | AdditionalInformation   | o      |         |

**E.5.5 MAPDU support**

The supplier of the implementation shall state support for the MAPDUs in the management role(s) for which conformance is claimed, in Table E.6.

**Table E.6 – MAPDU support**

| Index | MAPDU name    | Status  |       | Support |       |
|-------|---------------|---------|-------|---------|-------|
|       |               | Manager | Agent | Manager | Agent |
| E.6.1 | serviceReport | o.2     | o.2   |         |       |
| E.6.2 | usageReport   | o.3     | o.3   |         |       |

If support for the serviceReport MAPDU in the agent role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.7. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

**Table E.7 — Service report MAPDU (sending)**

| Index       | Parameter name          | Sts | Value | Spt | TVR |
|-------------|-------------------------|-----|-------|-----|-----|
| E.7.1       | SecurityAuditInfo       | —   | —     | —   | —   |
| E.7.1.1     | serviceReportCause      | m   |       |     |     |
| E.7.1.2     | notificationIdentifier  | c1  |       |     |     |
| E.7.1.3     | correlatedNotifications | o   |       |     |     |
| E.7.1.3.1   | correlatedNotifications | m   |       |     |     |
| E.7.1.3.2   | sourceObjectInst        | o   |       |     |     |
| E.7.1.3.2.1 | distinguishedName       | o.4 |       |     |     |
| E.7.1.3.2.2 | nonSpecificForm         | o.4 |       |     |     |
| E.7.1.3.2.3 | localDistinguishedName  | o.4 |       |     |     |
| E.7.1.4     | additionalText          | c2  |       |     |     |
| E.7.1.5     | additionalInformation   | c2  |       |     |     |
| E.7.1.5.1   | identifier              | m   |       |     |     |
| E.7.1.5.2   | significance            | m   |       |     |     |
| E.7.1.5.3   | information             | m   |       |     |     |

If support for the serviceReport MAPDU in the manager role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.8. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

**Table E.8 – Service report MAPDU (receiving)**

| Index       | Parameter name          | Sts | Value | Spt | TVR |
|-------------|-------------------------|-----|-------|-----|-----|
| E.8.1       | SecurityAuditInfo       | –   | –     | –   | –   |
| E.8.1.1     | serviceReportCause      | m   |       |     |     |
| E.8.1.2     | notificationIdentifier  | m   |       |     |     |
| E.8.1.3     | correlatedNotifications | m   |       |     |     |
| E.8.1.3.1   | correlatedNotifications | m   |       |     |     |
| E.8.1.3.2   | sourceObjectInst        | m   |       |     |     |
| E.8.1.3.2.1 | distinguishedName       | m   |       |     |     |
| E.8.1.3.2.2 | nonSpecificForm         | m   |       |     |     |
| E.8.1.3.2.3 | localDistinguishedName  | m   |       |     |     |
| E.8.1.4     | additionalText          | m   |       |     |     |
| E.8.1.5     | additionalInformation   | m   |       |     |     |
| E.8.1.5.1   | identifier              | m   |       |     |     |
| E.8.1.5.2   | significance            | m   |       |     |     |
| E.8.1.5.3   | information             | m   |       |     |     |

If support for the usageReport MAPDU in the agent role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.9. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

**Table E.9 – Usage report MAPDU (sending)**

| Index       | Parameter name          | Sts | Value | Spt | TVR |
|-------------|-------------------------|-----|-------|-----|-----|
| E.9.1       | SecurityAuditInfo       | –   | –     | –   | –   |
| E.9.1.1     | serviceReportCause      | –   | –     | –   | –   |
| E.9.1.2     | notificationIdentifier  | c1  |       |     |     |
| E.9.1.3     | correlatedNotifications | o   |       |     |     |
| E.9.1.3.1   | correlatedNotifications | m   |       |     |     |
| E.9.1.3.2   | sourceObjectInst        | o   |       |     |     |
| E.9.1.3.2.1 | distinguishedName       | o.5 |       |     |     |
| E.9.1.3.2.2 | nonSpecificForm         | o.5 |       |     |     |
| E.9.1.3.2.3 | localDistinguishedName  | o.5 |       |     |     |
| E.9.1.4     | additionalText          | c2  |       |     |     |
| E.9.1.5     | additionalInformation   | c2  |       |     |     |
| E.9.1.5.1   | identifier              | m   |       |     |     |
| E.9.1.5.2   | significance            | m   |       |     |     |
| E.9.1.5.3   | information             | m   |       |     |     |

If support for the usageReport MAPDU in the manager role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.10. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

Table E.10 – Usage report MAPDU (receiving)

| Index        | Parameter name          | Sts | Value | Spt | TVR |
|--------------|-------------------------|-----|-------|-----|-----|
| E.10.1       | SecurityAuditInfo       | –   | –     | –   | –   |
| E.10.1.1     | serviceReportCause      | –   | –     | –   | –   |
| E.10.1.2     | notificationIdentifier  | m   |       |     |     |
| E.10.1.3     | correlatedNotifications | m   |       |     |     |
| E.10.1.3.1   | correlatedNotifications | m   |       |     |     |
| E.10.1.3.2   | sourceObjectInst        | m   |       |     |     |
| E.10.1.3.2.1 | distinguishedName       | m   |       |     |     |
| E.10.1.3.2.2 | nonSpecificForm         | m   |       |     |     |
| E.10.1.3.2.3 | localDistinguishedName  | m   |       |     |     |
| E.10.1.4     | additionalText          | m   |       |     |     |
| E.10.1.5     | additionalInformation   | m   |       |     |     |
| E.10.1.5.1   | identifier              | m   |       |     |     |
| E.10.1.5.2   | significance            | m   |       |     |     |
| E.10.1.5.3   | information             | m   |       |     |     |

**Annex F**  
**Relationship with the security audit framework**

(This annex does not form an integral part of this Recommendation | International Standard)

This Recommendation | International Standard provides facilities for the logging of security-related events that are of potential use in a security audit. It does not define a security audit nor how to perform one. This Recommendation | International Standard is just one of the facilities that may be used to record security-related events that may be of interest to a security audit.

ISO/IEC 10181-7 defines the concepts and goals of a security audit and provides a description of security auditing functions. Thus, ISO/IEC 10181-7 describes what can be done with information associated with security-related events; not how to record that information.