

INTERNATIONAL STANDARD

ISO/IEC 10164-8

First edition
1993-06-15

Information technology — Open Systems Interconnection — Systems Management: Security audit trail function

iTeh STANDARD PREVIEW

*Technologies de l'information — interconnexion de systèmes ouverts
Gestion-système: Fonction de sécurité de l'expertise de l'historique*

ISO/IEC 10164-8:1993

<https://standards.iteh.ai/catalog/standards/sist/7571210c-7abf-4d08-a3b9-94809b4cfa8d/iso-iec-10164-8-1993>



Reference number
ISO/IEC 10164-8:1993(E)

Contents

	Page
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 function 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

© ISO/IEC 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 publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

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

iTeh STANDARD PREVIEW

Annexes

(standards.iteh.ai)

A	Definition of management information	12
B	MCS proforma.....	14
C	MOCS proforma	16
D	MIDS (notification) proforma	19
E	PICS proforma	20
F	Relationship with the security audit framework	26

Foreword

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

International Standard ISO/IEC 10164-8 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in collaboration with the CCITT. The identical text is published as CCITT Recommendation X.740.

ISO/IEC 10164 consists of the following parts, under the general title *Information technology – Open Systems Interconnection – Systems Management* :

- *Part 1: Object management function*
- *Part 2: State management function*
- *Part 3: Attributes for representing relationships*
- *Part 4: Alarm reporting function*
- *Part 5: Event report management function*
- *Part 6: Log control function*
- *Part 7: Security alarm reporting function*
- *Part 8: Security audit trail function*
- *Part 9: Objects and attributes for access control*
- *Part 10: Accounting meter function*
- *Part 11: Workload monitoring function*
- *Part 12: Test management function*
- *Part 13: Summarization function*
- *Part 14: Confidence and diagnostic test categories*

Annexes A, B, C, D and E form an integral part of this part of ISO/IEC 10164. Annex F is for information only.

Introduction

ISO/IEC 10164 is a multipart standard developed according to ISO 7498 and ISO/IEC 7498-4. ISO/IEC 10164 is related to the following International Standards

- ISO/IEC 9595 : 1991, *Information technology – Open Systems Interconnection – Common management information service definition*;
- ISO/IEC 9596 : 1991, *Information technology – Open Systems Interconnection – Common management information protocol*;
- ISO/IEC 10040 : 1992, *Information technology – Open Systems Interconnection – Systems management overview*;
- ISO/IEC 10165 : 1992, *Information technology – Open Systems Interconnection – Structure of management information*.

<https://standards.iteh.ai/catalog/standards/sist/7571210c-7abf-4d08-a3b9-94809b4cfa8d/iso-iec-10164-8-1993>

iTeh STANDARD PREVIEW

(standards.iteh.ai)

This page intentionally left blank

ISO/IEC 10164-8:1993

<https://standards.iteh.ai/catalog/standards/sist/7571210c-7abf-4d08-a3b9-94809b4cfa8d/iso-iec-10164-8-1993>

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.724¹⁾ | ISO/IEC 10165-6¹⁾, *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.*

¹⁾ Presently at the stage of draft.

- CCITT Recommendation X.710 (1991), *Common management information service definition for CCITT applications*.
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 10181-7¹⁾, *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.

¹⁾ 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.

ITeh STANDARD PREVIEW
(standards.iteh.ai)

4 Abbreviations

ASN.1	Abstract Syntax Notation One	ISO/IEC 10164-8:1993
CMIS	Common Management Information Services	https://standards.iteh.ai/catalog/standards/sist/7571210c-7abf-4d08-a3b9-9480704c1a0d/iso-iec-10164-8-1993
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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.