

STANDARD

10181-7

First edition
1996-08-01

**Information technology — Open Systems
Interconnection — Security frameworks for
open systems: Security audit and alarms
framework**

*Technologies de l'information — Interconnexion de systèmes ouverts
(OSI) — Cadres pour la sécurité dans les systèmes ouverts: Cadre pour
l'audit de sécurité et les alarmes*



This is a preview of "ISO/IEC 10181-7:1996". [Click here to purchase the full version from the ANSI store.](#)

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
3 Definitions.....	2
3.1 Basic Reference Model definitions	2
3.2 Security architecture definitions	2
3.3 Management framework definitions	3
3.4 Security framework overview definitions.....	3
3.5 Additional definitions	3
4 Abbreviations	4
5 Notation.....	4
6 General discussion of security audit and alarms	4
6.1 Model and functions	4
6.2 Phases of security audit and alarms procedures.....	6
6.3 Correlation of audit information	8
7 Policy and other aspects of security audit and alarms	8
7.1 Policy	8
7.2 Legal aspects	8
7.3 Protection requirements	8
8 Security audit and alarms information and facilities	9
8.1 Audit and alarms information	9
8.2 Security audit and alarms facilities	10
9 Security audit and alarms mechanisms	11
10 Interaction with other security services and mechanisms	12
10.1 Entity authentication	12
10.2 Data origin authentication.....	12
10.3 Access Control.....	12
10.4 Confidentiality	12
10.5 Integrity.....	12
10.6 Non-repudiation	12
Annex A – General security audit and alarms principles for OSI	13
Annex B – Realization of the security audit and alarm model	15
Annex C – Security Audit and Alarms Facilities Outline	17
Annex D – Time Registration of Audit Events	18

This is a preview of "ISO/IEC 10181-7:1996". [Click here to purchase the full version from the ANSI store.](#)

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 10181-7 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 21, *Open systems interconnection, data management and open distributed processing*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.816.

ISO/IEC 10181 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — Security frameworks for open systems*:

—Part 1: *Overview*

—Part 2: *Authentication framework*

—Part 3: *Access control framework*

—Part 4: *Non-repudiation framework*

—Part 5: *Confidentiality framework*

—Part 6: *Integrity framework*

—Part 7: *Security audit and alarms framework*

Annexes A to D of this part of ISO/IEC 10181 are for information only.

This is a preview of "ISO/IEC 10181-7:1996". [Click here to purchase the full version from the ANSI store.](#)

Introduction

This Recommendation | International Standard refines the concept of security audit described in ITU-T Rec. X.810 | ISO/IEC 10181-1. This includes event detection and actions resulting from these events. The framework, therefore, addresses both security audit and security alarms.

A security audit is an independent review and examination of system records and activities. The purposes of a security audit include:

- assisting in the identification and analysis of unauthorized actions or attacks;
- helping ensure that actions can be attributed to the entities responsible for those actions;
- contributing to the development of improved damage control procedures;
- confirming compliance with established security policy;
- reporting information that may indicate inadequacies in system controls; and
- identifying possible required changes in controls, policy and procedures.

In this framework, a security audit consists of the detection, collection and recording of various security-related events in a security audit trail and analysis of those events.

Both audit and accountability require that information be recorded. A security audit ensures that sufficient information is recorded about both routine and exceptional events so that later investigations can determine if security violations have occurred and, if so, what information or other resources have been compromised. Accountability ensures that relevant information is recorded about actions performed by users, or processes acting on their behalf, so that the consequences of those actions can later be linked to the user(s) in question, and the user(s) can be held accountable for his or her actions. Provision of a security audit service can contribute to the provision of accountability.

A security alarm is a warning issued to an individual or process to indicate that a situation has arisen that may require timely action. The purposes of a security alarm service include:

- to report real or apparent attempts to violate security;
- to report various security-related events, including “normal” events; and
- to report events triggered by threshold limits being reached.