INTERNATIONAL STANDARD

ISO/IEC 19770-1

Third edition
2017-12

Information technology — IT asset management —

Part 1: IT asset management systems — Requirements

Technologies de l'information — Gestion des actifs logiciels — Partie 1: Procédés et évaluation progressive de la conformité

Reference number
ISO/IEC 19770-1:2017(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**
1.1 Purpose 1
1.2 Field of application 1
1.3 Limitations 1

2 Normative references **2**

3 Terms and definitions **2**

4 Context of the organization **12**
4.1 Understanding the organization and its context 12
4.2 Understanding the needs and expectations of stakeholders 12
4.3 Determining the scope of the IT asset management system 13
4.4 IT asset management system 13

5 Leadership **13**
5.1 Leadership and commitment 13
5.2 Policy 14
5.3 Organizational roles, responsibilities and authorities 14

6 Planning **15**
6.1 Actions to address risks and opportunities for the IT asset management system 15
6.1.1 General 15
6.1.2 IT asset risk assessment 15
6.1.3 IT asset risk treatment 16
6.2 IT asset management objectives and planning to achieve them 16
6.2.1 IT asset management operation process specification 16
6.2.2 IT asset management objectives for operation processes 17
6.2.3 Overall IT asset management objectives 17
6.2.4 Planning to achieve IT asset management objectives 17

7 Support **18**
7.1 Resources 18
7.2 Competence 18
7.3 Awareness 19
7.4 Communication 19
7.5 Information requirements 19
7.6 Documented information 20
7.6.1 General 20
7.6.2 Traceability of ownership and responsibility 20
7.6.3 Audit trails of authorizations and execution of authorizations 21
7.6.4 Creating and updating 21
7.6.5 Control of documented information 21

8 Operation **22**
8.1 Operational planning and control 22
8.2 Management of change 22
8.3 Core data management 22
8.4 License management 22
8.5 Security management 23
8.6 Other processes 23
8.7 Outsourcing and services 23
8.8 Mixed responsibilities between the organization and its personnel 24

9 Performance evaluation **24**
9.1 Monitoring, measurement, analysis and evaluation 24
9.2 Internal audit 25

9.3 Management review 25
10 Improvement 26
10.1 Nonconformity and corrective action 26
10.2 Preventive action 26
10.3 Continual improvement 26
Annex A (normative) **IT asset management operation processes and objectives 27**
Annex B (informative) **IT asset management tiers 31**
Annex C (informative) **Characteristics of IT Assets 33**
Annex D (informative) **Changes from ISO 55001 ..... 35**
Bibliography 37

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and system engineering*. Participation and contributions were requested in particular from ISO/IEC JTC 1/SC 27 *IT Security Techniques*, ISO/IEC JTC 1/SC 40 *IT Service Management and IT Governance*, and ISO/TC 251 *Asset Management*.

This third edition cancels and replaces the second edition (ISO/IEC 19770-1:2012), which has been technically revised to be a Management System Standard.

A list of all parts in the ISO/IEC 19770 series can be found on the ISO website.

Introduction

This document specifies the requirements for the establishment, implementation, maintenance and improvement of a management system for IT asset management (ITAM), referred to as an "IT asset management system" (ITAMS).

This document provides additional requirements to ISO 55001:2014 which specifies the requirements for the establishment, implementation, maintenance and improvement of a management system for asset management, referred to as an "asset management system". This document includes additional or more detailed requirements which are considered necessary for the management of IT assets. The primary differentiator is the need to manage software assets, with their specific characteristics. Although ISO 55001:2014 can be used to manage software assets if organizations define their scope and relevant requirements appropriately, it is primarily focused on physical assets with little provision for the management of software assets.

There are a number of characteristics of IT assets which create these additional or more detailed requirements. These are described in Annex C. As a result of these characteristics of IT assets, a management system for IT assets will consequently have explicit requirements additional to those in ISO 55001:2014 dealing with:

— controls over software modification, duplication and distribution, with particular emphasis on access and integrity controls;

— audit trails of authorizations and of changes made to IT assets;

— controls over licensing, underlicensing, overlicensing, and compliance with licensing terms and conditions;

— controls over situations involving mixed ownership and responsibilities, such as in cloud computing and with 'Bring-Your-Own-Device' (BYOD) practices; and

— reconciliation of IT asset management data with data in other information systems when justified by business value, in particular with financial information systems recording assets and expenses.

Furthermore, because information associated with IT assets is typically voluminous, highly complex and fast-changing, it is likely that organizations with such information will need to make use of automated information systems.

Another difference between ISO 55001:2014 and this document is that this document provides optionally for multiple explicit groupings of process objectives (or 'tiers'). The most important of these is the basic tier called 'trustworthy data', which is the most important to most end-user organizations and also software publishers. Tier two is for 'life cycle integration', and tier three is for 'optimization'. More information about the tiers and their respective groupings of objectives is given in Annex B.

Since major physical assets increasingly incorporate or depend on software, it is likely that the additional requirements of this document will be relevant in such situations. It is likely that most organizations with major physical assets will need management systems meeting a mixture of 'pure' ISO 55001:2014 requirements and also of the additional requirements from this document.

IT assets encompass a wide variety of asset types. Figure 1 indicates the principal IT asset types diagrammatically.

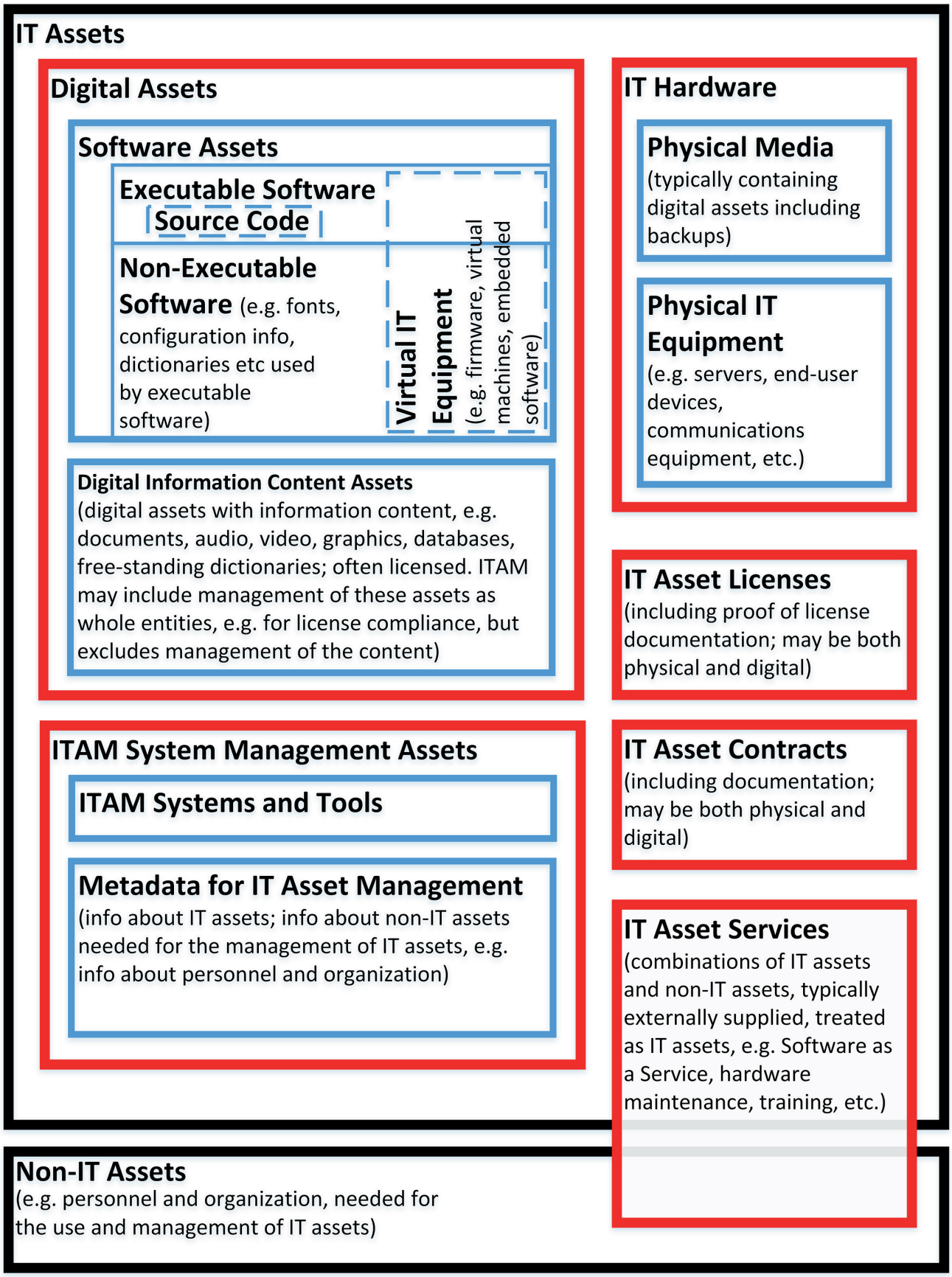

Figure 1 — Principal types of IT assets

This document can be used by any organization and can be applied to all types of IT assets. The organization determines to which of its IT assets this document applies.

This document is primarily intended for use by:

— those involved in the establishment, implementation, maintenance, and improvement of an IT asset management system;

— those involved in delivering IT asset management activities, including service providers;

— internal and external parties to assess the organization's ability to meet legal, regulatory and contractual requirements and the organization's own requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented.

Further guidance regarding the application of the requirements within this document shared with ISO 55001:2014 is provided in ISO 55002.

General information on asset management and on IT asset management, and information on the terminology applicable to this document, is provided in ISO 55000 and in ISO/IEC 19770-5. Organizations can find that these documents will assist in the development of IT asset management in their organization.

This document applies the definition of "risk" given in ISO 31000:2009 and ISO/IEC Guide 73:2009. In addition, it uses the term "stakeholder" rather than "interested party".

This document is designed to enable an organization to align and integrate its IT asset management system with related management system requirements, for example those specified by ISO/IEC 27001 and ISO/IEC 20000-1.

This document is not intended to be in conflict with any organization's policies, procedures and standards. Any such conflict should be resolved before using this document.

Information technology — IT asset management —

Part 1:
IT asset management systems — Requirements

1 Scope

1.1 Purpose

This document specifies requirements for an IT asset management system within the context of the organization.

This document can be applied to all types of IT assets and by all types and sizes of organizations.

NOTE 1 This document is intended to be used for managing IT assets in particular, but it can also be applied to other asset types. It can be suitable, in whole or in part, for managing embedded software and firmware, however its use for these purposes has not been determined. It is not intended for managing information assets per se, i.e. it is not intended for managing information as an asset independent of hardware and software assets. Certain types of data and information are covered, such as data and information about IT assets in scope, and depending on how the scope is defined, it can cover digital information content assets. See the Introduction for an explanation about IT assets.

NOTE 2 This document does not specify financial, accounting, or technical requirements for managing specific IT asset types.

NOTE 3 For the purposes of this document, the term "IT asset management system" is used to refer to a management system for IT asset management.

This document is a discipline-specific extension of ISO 55001:2014, with changes, and is not a sector-specific application of that International Standard. ISO 55001:2014 is intended to be used for managing physical assets in particular, but it can also be applied to other asset types. This document specifies requirements for the management of IT assets which are additional to those specified in ISO 55001:2014. Conformance to this document does not imply conformance to ISO 55001:2014.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own IT asset management requirements.

1.2 Field of application

This document applies to IT asset management processes and can be implemented by organizations to achieve immediate benefits.

This document can be applied to all IT assets. For example, it can be applied to not only IT hardware but also to executable software (such as application programs and operating systems) and non-executable software (such as fonts and configuration information). It can be applied to all technological environments and computing platforms (e.g. virtualized software applications, on-premises or software-as-a-service; it is equally relevant in cloud computing as it is in legacy computing environments).

1.3 Limitations

This document does not detail the IT asset management processes in terms of methods or procedures required to meet the requirements for outcomes of a process.

This document does not specify the sequence of steps an organization should follow to implement IT asset management.

This document does not detail documentation in terms of name, format, explicit content and recording media.

2 Normative references

There are no normative references in this document.