INTERNATIONAL STANDARD

ISO/IEC 19770-5

Second edition
2015-08-01

Information technology — IT asset management — Overview and vocabulary

Technologies de l'information — Gestion de biens de logiciel — Vue d'ensemble et vocabulaire

Reference number
ISO/IEC 19770-5:2015(E)

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 IT asset management (ITAM) and software asset management (SAM) ... **8**
4.1 Introduction ... 8
4.2 The need to manage software assets ... 9
4.2.1 General ... 9
4.2.2 Direct benefits ... 9
4.2.3 Cost control ... 10
4.2.4 Risk management and mitigation ... 10
4.3 Foundation principles ... 11
4.4 Relationships to principles defined in other standards ... 11
4.4.1 Introduction ... 11
4.4.2 Relationship to ISO 9001 principles ... 11
4.4.3 Relationship to ISO/IEC 20000 principles ... 11
4.4.4 Relationship to ISO/IEC 27000 principles ... 11
4.4.5 Relationship to ISO 55000 principles ... 12
4.5 Principles of process definitions ... 12
4.6 Evaluation of process definition conformance ... 12
4.7 Principles of information structures ... 13
4.8 Evaluation of information structure definition conformance ... 13
4.9 Critical success factors ... 13
5 ITAM family of standards ... **14**
5.1 General information ... 14
5.2 Standards specifying processes ... 14
5.2.1 ISO/IEC 19770-1:2006 ... 14
5.2.2 ISO/IEC 19770-1:2012 ... 15
5.2.3 ISO/IEC 19770-1:201x ... 15
5.3 Technical reports providing guidance for process standards ... 15
5.3.1 ISO/IEC 19770-8:201x ... 15
5.3.2 ISO/IEC 19770-11:201x ... 15
5.4 Standards specifying information structures ... 16
5.4.1 ISO/IEC 19770-2:2009 ... 16
5.4.2 ISO/IEC 19770-2:201x ... 16
5.4.3 ISO/IEC 19770-3:201x ... 16
5.4.4 ISO/IEC 19770-4:201x ... 17
5.4.5 ISO/IEC 19770-6:201x ... 17
5.5 Technical reports providing guidance for information structure standards ... 17
5.5.1 ISO/IEC 19770-7:201x ... 17
5.5.2 ISO/IEC 19770-22:201x ... 17
5.6 Overview standards ... 18
5.6.1 ISO/IEC 19770-5:2013 ... 18
5.6.2 ISO/IEC 19770-5:2015 (this standard) ... 18
Bibliography ... **19**

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

This second edition cancels and replaces the first edition (ISO/IEC 19770-5:2013), which has been technically revised.

ISO/IEC 19770 consists of the following parts, under the general title *Information technology — Software asset management*:

— *Part 1: Processes and tiered assessment of conformance*

— *Part 2: Software identification tag*

— *Part 3: Software entitlement schema*

— *Part 5: Overview and vocabulary*

The following parts are under preparation:

— *Part 4: Resource Utilization Measurement (RUM)*

— *Part 7: Tag management*

Introduction

Overview

International Standards in the ISO/IEC 19770 family of standards for software asset management (SAM) address both the processes and technology for managing software assets and related IT assets. Because IT is an essential enabler for almost all activity in today's world, these standards must integrate tightly into all of IT. For example, from a process perspective, SAM standards must be able to be used with all Management System Standards, because software and software management are essential components of any modern Management System. From a technology perspective, SAM standards for information structures provide not only for data interoperability of software management data, but also provide the basis for many related benefits such as more effective security in the use of software. SAM standards for information structures also facilitate significant automation of IT functionality, such as improved authentication of software and linking to national vulnerability databases for more automated exposure identification and mitigation.

SAM family of standards

The ISO/IEC 19770 family of standards is intended to assist organizations of all types to implement and operate a software asset management system using both process and technology. The ISO/IEC 19770 family of standards consists of the parts listed in the Foreword.

NOTE ISO/IEC 19770-4, ISO/IEC 19770-6, ISO/IEC 19770-9 and ISO/IEC 19770-10 are either related to projects that have been withdrawn, or are reserved for future use.

Purpose of this part of ISO/IEC 19770

This part of ISO/IEC 19770 provides an overview of software asset management, which is the subject of the ISO/IEC 19770 family of standards, and defines related terms.

This part of ISO/IEC 19770 is divided into the following clauses:

— Clause 1 is the scope;

— Clause 2 describes the normative references;

— Clause 3 describes the terms, definitions, symbols, and abbreviations;

— Clause 4 introduces software asset management, describes the alignment of SAM standards with other ISO and ISO/IEC standards, and defines principles of SAM processes and data structures;

— Clause 5 gives an overview of the SAM standards family.

The terms and definitions provided in this part of ISO/IEC 19770

a) cover commonly used terms and definitions in the ISO/IEC 19770 family of standards,

b) will not cover all terms and definitions applied within the ISO/IEC 19770 family of standards, and

c) do not limit the ISO/IEC 19770 family of standards in defining terms for their own use.

To reflect the changing status of the SAM family of standards, this part of ISO/IEC 19770 is expected to be updated on a more frequent basis than would normally be the case for other ISO/IEC standards.

Information technology — IT asset management — Overview and vocabulary

1 Scope

This part of ISO/IEC 19770 provides

a) an overview of the ISO/IEC 19770 family of standards,

b) an introduction to IT asset management (ITAM) and software asset management (SAM),

c) a brief description of the foundation principles and approaches on which SAM is based, and

d) consistent terms and definitions for use throughout the ISO/IEC 19770 family of standards.

This part of ISO/IEC 19770 is applicable to all types of organization (e.g. commercial enterprises, government agencies, and non-profit organizations).

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 55000:2014, *Asset management — Overview, principles and terminology*

RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*, January 2005[1)]

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
application
system for collecting, saving, processing, and presenting data by means of a computer.

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.119, definition 1]

3.2
asset
item, thing, or entity that has potential or actual value to an organization

Note 1 to entry: Value can be tangible or intangible, financial, or non-financial, and includes consideration of risks and liabilities. It can be positive or negative at different stages of the asset life.

Note 2 to entry: Physical assets usually refer to equipment, inventory, and properties owned by the organization. Physical assets are the opposite of intangible assets, which are non-physical assets such as leases, brands, digital assets, use rights, licences, intellectual property rights, reputation, or agreements.

Note 3 to entry: A grouping of assets referred to as an asset system could also be considered as an asset.

Note 4 to entry: ISO/IEC 19770-5:2013 incorporated a slightly different definition of asset, taken from a development version of ISO 55000. This definition is sourced from the published version.

1) http://tools.ietf.org/html/rfc3986

[SOURCE: ISO 55000:2014, 3.2.1, modified—Note 4 has been added.]

3.3
asset management
coordinated activity of an organization to realize value from *assets* (3.2)

[SOURCE: ISO 55000:2014, 3.3.1, modified — The Notes have been deleted.]

3.4
baseline
formally approved version of a *configuration item* (3.7), regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.240, definition 2]

3.5
bundle
grouping of products which is the result of a marketing/licensing strategy to sell entitlements to multiple products as one purchased item

Note 1 to entry: A bundle can be referred to as a "suite", if the products are closely related and typically integrated (such as an office suite containing a spreadsheet, word processor, presentation, and other related items).

Note 2 to entry: Bundles can also refer to software titles that are less closely related such as a game, a virus scanner and a utility "bundled" together with a new computer, or to groups of entitlements, such as multiple entitlements for a backup software product.

3.6
computing device
functional unit that can perform substantial computations, including numerous arithmetic operations and logic operations with or without human intervention

Note 1 to entry: A computing device can consist of a stand-alone unit, or several interconnected units. It can also be a device that provides a specific set of functions, such as a phone or a personal organizer, or more general functions such as a laptop or desktop computer.

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.513 (computer), modified — "with or" has been added to the definition.]

3.7
configuration item
CI
component of an infrastructure or an item which is or will be, under control of configuration management

Note 1 to entry: Configuration items may vary widely in complexity, size and type, ranging from an entire system including all hardware, software and documentation, to a single module or a minor hardware component.

Note 2 to entry: Configuration items are commonly defined as part of service management practice and can vary widely in complexity, size, and type, ranging from an entire system including all hardware, software and documentation, to a single module or a minor hardware component.

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.563, definition 3, modified — Note 2 to entry has been added]

3.8
configuration management database
CMDB
database containing all the relevant details of each *configuration item* (3.7) and details of the important relationships between them

Note 1 to entry: When aligning service management with SAM, it may be convenient for the organization to ensure that CIs cover all software within the scope of SAM, i.e. it may be an advantage for anticipated manifestations of controlled/licensed software usage to be fully mapped to CIs and so accountable through all the service management processes using CIs.

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.566, modified — Note 1 to entry has been added.]

3.9
corporate board or equivalent body
person or group of people who assumes legal responsibility for conducting or controlling an organization at the highest level

3.10
customer
organization or person that receives a product or service

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.696, definition 1]

3.11
definitive software library
DSL
secure storage environment, formed of physical media, or of one or more electronic software repositories, capable of control and protection of definitive authorized versions of all software *configuration items* (3.7) and masters of all software controlled by *SAM* (3.35)

3.12
element
component of a *{info struct}* (3.18) that provides information related to the entity represented by the {info struct}

3.13
end-user
person or persons who will ultimately be using the system for its intended purpose

Note 1 to entry: In the ISO/IEC 19770 family of standards, an end user will generally be defined in terms of a specific *software component* (3.36) of a system.

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.990 (end user), definition 1, modified — Note 1 to entry has been added.]

3.14
entitlement
see *software entitlement* (3.39)

3.15
extensible markup language
XML
license-free and platform-independent markup language that carries rules for generating text formats that contain structured data

[SOURCE: W3C Recommendation *Extensible Markup Language (XML) 1.1 (Second Edition)*, 1.2]

3.16
globally unique identifier
GUID
16-byte string of characters that is generated in a manner that gives a high probability that the string is unique in any context

Note 1 to entry: Other globally unique identifier algorithms can be used in some situations. In general, alternative algorithms use Uniform Resource Identifier (URI) based structures, so the id owner's registration identifier (regid) is included in the identifier.

Note 2 to entry: In this part of ISO/IEC 19770, GUID as an all capitalized term refers specifically to the 16 byte version. If the term is in lowercase (guid), it refers to a general algorithm that can use either a URI, or a 16-byte-based identifier.

3.17
legacy software
software (3.34) originally created without {info struct}s

3.18
information structure
{info struct}
structure that provides information about a software *asset* (3.2) in order to facilitate its management

Note 1 to entry: {info struct} is a placeholder used in these terms and definitions to provide a generic reference to all information structures defined within the 19770 family of standards. However individual standards are free to use a descriptive term that reflects their specific usage, and to use the terms and definitions defined herein with {info struct} replaced by that term. For example, the software identification information structure is named a *SWID tag* (3.40).

3.19
{info struct} creator
entity that initially creates an *{info struct}* (3.18)

Note 1 to entry: This entity can be part of the organization that created the software, in which case the {info struct} creator and software creator will be the same. The {info struct} creator can also be a third party organization unrelated to the software creator (such as in the case where {info struct}s are created for legacy software by third party organizations).

3.20
{info struct}Id
value that shall be globally unique for every *{info struct}* (3.18) created

3.21
local SAM owner
individual at a level of the organization below that of the *SAM owner* (3.30) who is identified as being responsible for SAM for a defined part of the organization

3.22
message digest 5
MD5
algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual

3.23
platform
type of computer or hardware device and/or associated operating system, or a virtual environment, on which software can be installed or run

Note 1 to entry: A platform is distinct from the unique instances of that platform, which are typically referred to as devices or instances.

3.24
primary {info struct}
{info struct} (3.18) to which supplemental {info struct}s may be linked

3.25
procedure
specified way to carry out an activity or process

Note 1 to entry: When a procedure is specified as an outcome, the resulting deliverable will typically specify what must be done, by whom, and in what sequence. This is a more detailed level of specification than for a *process* (3.26).

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.2216, definition 4, modified — Note 1 to entry has been added.]

3.26
process
set of interrelated or interacting activities, which transforms inputs into outputs

Note 1 to entry: When a process definition is specified as an outcome, the resulting deliverable will typically specify inputs and outputs, and give a general description of expected activities. However, it does not require the same level of detail as for a *procedure* (3.25).

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.2217, definition 1, modified — Note 1 to entry has been added.]

3.27
registration identifier
regid
unique identifier for an entity

Note 1 to entry: ISO/IEC 19770-5:2013 incorporated a different definition of *regid* that defined a specific format.

3.28
release
collection of one or more new or changed configuration items deployed into the live environment as a result of one or more changes

[SOURCE: ISO/IEC 20000-1:2011, 3.2.3]

3.29
reseller
organization that purchases goods or services with an intention of selling them to another customer and possibly supporting them

3.30
SAM owner
individual at a senior organization-wide level who is identified as being responsible for *SAM* (3.35)

3.31
SAM practitioner
individual involved in the practice or role of managing software assets

Note 1 to entry: A SAM practitioner is often involved in the collection or reconciliation of software inventory and/or software entitlements.

3.32
SAM program scope
clear statement listing of all parts of the organization and types of software, assets, platforms, etc. covered by a SAM program

3.33
secure hash algorithm
SHA
algorithm that is used to verify data integrity through the creation of a message digest from data input (which may be a message of any length), with SHA-1 (160 bit digest) in current widespread use, and SHA-2 (224 to 512 bit digest) starting to be deployed

3.34
software
all or part of the programs, procedures, rules, and associated documentation of an information processing system

Note 1 to entry: There are multiple definitions of software in use. For the purposes of this part of ISO/IEC 19770, it is typically important to include both executable and non-executable software, such as fonts, graphics, audio and video recordings, templates, dictionaries, documents and information structures such as database records.

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.2741, definition 1, modified – Note 1 to entry has been added.]