INTERNATIONAL STANDARD

ISO/IEC 19770-1

Second edition
2012-06-15

Information technology — Software asset management —

Part 1: Processes and tiered assessment of conformance

Technologies de l'information — Gestion de biens de logiciel —

Partie 1: Procédés et évaluation progressive de la conformité

Reference number
ISO/IEC 19770-1:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

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.

ISO/IEC 19770-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and system engineering*.

This second edition cancels and replaces the first edition (ISO/IEC 19770-1:2006), 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*

The following parts are under preparation:

— *Part 3: Software entitlement tag*

— *Part 5: Overview and vocabulary*

Part 5 will define a common set of vocabulary for the ISO/IEC 19770 series, which may update definitions given in previously published parts.

Tag management will form the subject of a future Part 7.

Introduction

This part of ISO/IEC 19770 is for organizations that want to achieve best practice in Software Asset Management (SAM). It grew out of ISO/IEC 19770-1:2006 *Software asset management processes* which was a comprehensive standard designed to align to all of service management as specified in ISO/IEC 20000.

However, market feedback was that organizations wanted something which could be accomplished in multiple increments and to that increment most suited to the needs of the organization. This part of ISO/IEC 19770 has been designed to make implementation of SAM and conformance to a published standard possible at any one of these increments, called “tiers”, which are cumulative. This allows for free-standing independent certification which correspond to natural levels of development and management priority. Recognition is given to those organizations through the ability to publicly display that certification has been achieved to a stated tier.

Division into tiers is designed so that standardized SAM is within reach of most organizations. Those implementing SAM for the first time can often implement SAM more rapidly by also applying careful scoping of the software assets covered and by scoping the parts of the organization covered by SAM. An organization will not normally cover everything possible in-scope and software scope and organizational scope definitions are allowed as described in Clause 1 Scope. Any scope may be defined so long as it is not ambiguous.

When an organization chooses to narrow the scope of SAM in this way, certain factors should be considered so that all desired benefits and objectives of the organization can be achieved. For example, for good security it is usually necessary for all assets within certain sections of an organization’s infrastructure to be included within the scope of SAM. Furthermore, it is impossible to manage software assets without also managing the hardware on which it runs and this part of ISO/IEC 19770 may be used for both. The term SAM is intended to cover all software-related assets within IT and use of the term SAM for this part of ISO/IEC 19770 reflects the organizational location of the responsible ISO/IEC Working Group and reflects market usage. SAM has wide ranging benefits across other interrelated practices of managing IT assets and implementers of good SAM practices can expect to attain benefits beyond management of the software itself.

The four tiers of SAM as defined in this part of ISO/IEC 19770 are shown in Figure 1. For a fuller description of the four tiers, see Clause 5 Tiers. They can be briefly explained as follows:

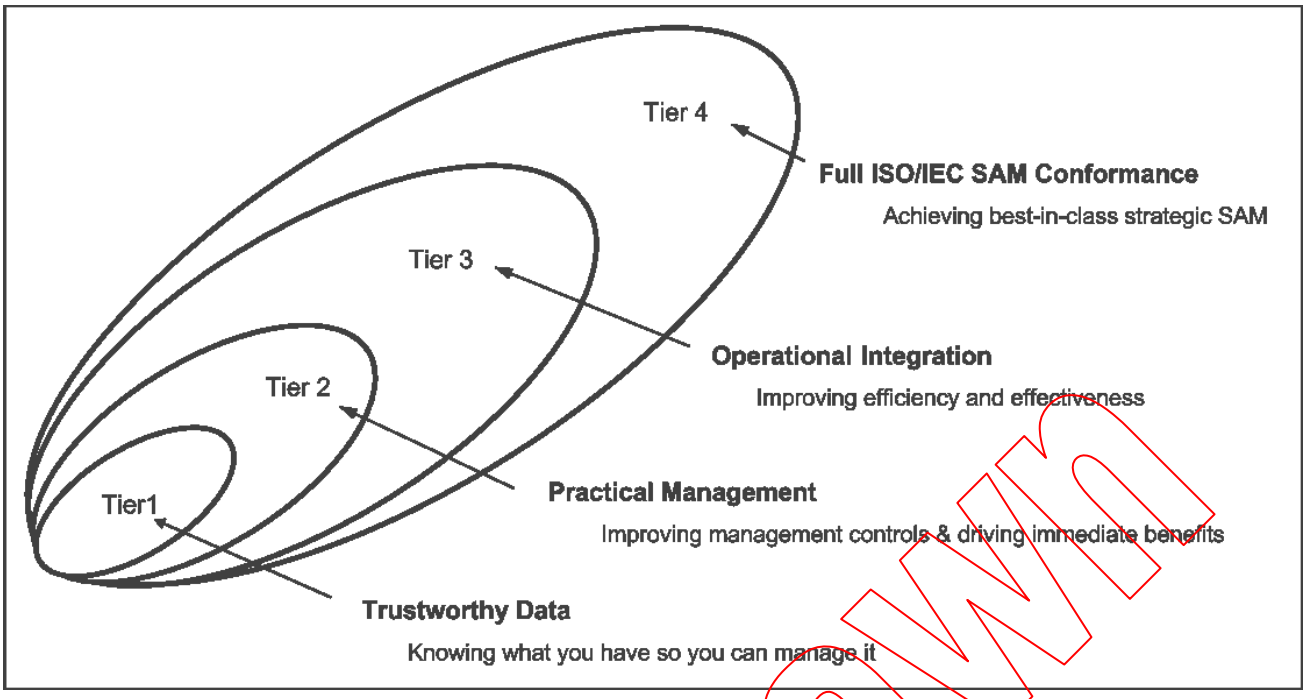

Figure 1 — The four tiers of SAM

The major associated benefits of each tier are:

- Tier 1: Trustworthy Data. Achieving this tier means knowing what you have so that you can manage it.

  Good data is a prerequisite for good SAM. A common management observation which applies here is that “you cannot manage what you do not know”. This tier also provides the basis for demonstrating license compliance, which is typically a high priority management objective.

  NOTE Other parts of ISO/IEC 19770 define a Software Identification Tag (ISO/IEC 19770-2), and a Software Entitlement Tag (ISO/IEC 19770-3) that are intended to simplify the task of achieving trustworthy data.

- Tier 2: Practical Management. Achieving this tier means improving management controls and driving immediate benefits.

  In practice, management typically only starts to take ownership of issues related to SAM after the organization has recognized the issues which result from not having trustworthy data. The organization recognizes the extent of the risks it faces as well as the opportunities for improvement and savings. This tier covers the basic management control environment (see 4.2 Control environment for SAM), including policies, roles and responsibilities. It also includes targeting and delivering “quick wins” made obvious by the data of Tier 1.

- Tier 3: Operational Integration. Achieving this tier means improving efficiency and effectiveness.

  Building on the foundation of the previous two tiers, this tier drives the integration of SAM into operational processes (see 4.6 Operations management processes and interfaces for SAM). The result is improved efficiency and effectiveness.

  NOTE Other parts of ISO/IEC 19770 define a Software Identification Tag (ISO/IEC 19770-2), and a Software Entitlement Tag (ISO/IEC 19770-3) that are designed to simplify the task of integration.

- Tier 4: Full ISO/IEC SAM conformance. Achieving this tier means achieving best-in-class strategic SAM.

  This tier addresses the more advanced and demanding aspects of full SAM, including its full integration into strategic planning for the organization.

The first three tiers are defined as subsets of the total set of process areas and outcomes defined in this part of ISO/IEC 19770, i.e. each process area has a single SAM objective, such as Software Asset Identification, and contains multiple outcomes for processes to support each objective. See Annex A for a summary table illustrating this structure.

The tiers build on one another with Tier 4 defined as the total set of process areas and outcomes defined in this part of ISO/IEC 19770. Note that the process areas and outcomes defined in this part of ISO/IEC 19770 are largely unchanged from ISO/IEC 19770-1:2006 but some minor clarifications have been included. The structure of process group objectives containing multiple outcomes has also been consistently maintained. Conformance may now be established to any specific tier. Although each can be certified separately, each relies on the continued performance of the previous tiers. In practical terms, this would typically mean that an organization going through a certification exercise for a higher tier would receive the usual review visit by the certifier for surveillance of any previous tier or tiers, and this same certifier visit would review the higher tier too.

A fuller explanation of the tiers and their makeup is given in Clause 5.

The overall benefits of SAM should include:

a) **Risk management**: for example mitigating interruption or deterioration of IT/services; legal and regulatory exposure;

b) **Cost control**: reduced direct costs of software and reduced direct costs of software, related assets (see 1.2 for a description of related assets) and ongoing support costs and contracts;

c) **Competitive advantage**: better business decisions and satisfaction from trustworthy data always at-hand.

Typically business requirements may mean targeting priority areas, such as for particular software manufacturers or sometimes for a specified group of organizational units. Choices of tiers, combined with scoping, allow for many organizations to benefit from standardized SAM processes as described in Clause 1 Scope.

In principle it would also be possible to use a capability or maturity approach to define a standard which can be accomplished in stages. In practice however, such an approach is significantly more complex if it is to be independently certifiable. This notwithstanding, it is intended to develop such an approach in the future, after a planned revision of the first edition of ISO/IEC 15504 is completed. This will allow for a convergence of approaches based on this part of ISO/IEC 19770 and on other methodologies in the marketplace based on maturity.

Information technology — Software asset management —

Part 1:
Processes and tiered assessment of conformance

1 Scope

1.1 Purpose

This part of ISO/IEC 19770 establishes a baseline for an integrated set of processes for Software Asset Management (SAM), divided into tiers to allow for incremental implementation, assessment and recognition.

1.2 Field of application

This part of ISO/IEC 19770 applies to SAM processes and can be implemented by organizations to achieve immediate benefits. ISO/IEC 19770-2 provides a corresponding specification for software identification tags, which requires implementation by software manufacturers (external and internal) and by tool developers for its full benefits to be achieved

It is intended that this part of ISO/IEC 19770 be an implementation standard for organizations. Future editions may provide a measurement framework that is aligned to the requirements in ISO/IEC 15504-2:2003 or the future International Standard ISO/IEC 33003[1].

This part of ISO/IEC 19770 applies to all organizations of any size or sector. For the purposes of conformance, this part of ISO/IEC 19770 can only be applied to a legal entity, or to parts of a single legal entity. It may also be applied to multiple legal entities (e.g. the parent and subsidiaries of a multinational organization) where there is a legal controlling relationship between them, so that one entity may exercise control over the others. It applies only where such a controlling entity exercises control over the entire scope (as defined for purposes of conformance) and the assessor of conformance accepts this definition of organizational scope.

NOTE The definition of organizational scope is documented as part of the *Corporate governance process for SAM* (4.2.2).

This part of ISO/IEC 19770 may be applied to an organization which has outsourced SAM processes, with the responsibility for demonstrating conformance always remaining with the outsourcing organization.

This part of ISO/IEC 19770 can be applied to all software and related assets, regardless of the nature of the software, where related assets are all other assets with characteristics which are necessary to use or manage software. For example, it can be applied to executable software (such as application programs, operating systems and utility programs) and to non-executable software (such as fonts, graphics, audio and video recordings, templates, dictionaries, documents and data). 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 older computing environments).

NOTE The definition of software asset scope (software types to be included within the scope) is documented as part of the SAM Plan developed in the *Planning for SAM* process. It may be defined in any way considered appropriate by the organization, such as for all software, for all program software, for all software on specific platforms, or for the software of specified manufacturers, as long as it is unambiguous. See also explanations following in this subclause and in Table 1.

1 ISO/IEC 33003, *Systems and software engineering — Requirements for process measurement frameworks*.

With the exception of the requirements of 4.7.4 Software development process, it is not required for this part of ISO/IEC 19770 to be applied to software development in the sense of the development and maintenance of code. It is intended that it be applied to all software in a live environment and precursor activities, such as configuring software and creating and controlling production builds and releases. The exact dividing line between what is considered pure development, and therefore excluded, and what is related to the live environment, and therefore included, may be defined making use of the unambiguous formal statements of organizational scope or software scope.

NOTE Software used to develop other software is considered part of the live environment, i.e. the software used by software developers must itself be controlled.

The following forms of software assets are within the scope of this part of ISO/IEC 19770:

a) software use rights, reflected by full ownership (as for in-house developed software) and licenses (as for most externally sourced software, whether commercial or open-source);

b) software for use, which contains the intellectual property value of software (including original software provided by software manufacturers and developers, software builds, and software as installed and otherwise provisioned, consumed or executed); and

c) media holding copies of software for use.

NOTE From a financial accounting point of view, it is primarily category (a) which may be considered an asset, and even then it may have been completely written off. From a financial accounting point of view, category (b) may be viewed as actually creating a liability (rather than an asset) with commercial software if it is not properly licensed. This part of ISO/IEC 19770 considers categories (b) and (c) proper assets to be controlled as well as (a). Licenses may have bookkeeping value, but software in use in particular should have business value and needs to be treated as a business asset.

Related assets within the scope are all other assets with characteristics which are necessary to use or manage software in scope. Any characteristics of these related assets which are not required to use or manage software are outside of the scope. Table 1 provides examples of these.

Table 1 — Application of ISO/IEC 19770-1 to Non-Software Assets

Asset type	*Applicability*	*Example*
Hardware	**Normative** for hardware assets with characteristics required for the use or management of software assets in scope	Inventory of equipment on which software can be stored, executed or otherwise used; number of processors or processing power; whether the hardware qualifies for counting for site licensing purposes
	Not applicable for characteristics not required for the use or management of software assets in scope	Cost and depreciation of hardware, preventive maintenance renewal dates
Other assets	**Normative** for other assets with characteristics required for the use or management of software assets in scope	Personnel names for identifying custodianship; personnel counts for licensing, where determined on this basis; IT infrastructure or architecture (including interfaces) if needed to determine the proper usage for certain license metrics, e.g. to identify multiplexing
	Not applicable for characteristics not required for the use or management of software assets in scope	Other personnel information

1.3 Limitations

This part of ISO/IEC 19770 does not detail the SAM processes in terms of methods or procedures required to meet the requirements for outcomes of a process.

This part of ISO/IEC 19770 does not specify the sequence of steps an organization should follow to implement SAM, nor is any sequence implied by the sequence in which processes are described. The only sequencing which is relevant is that which is required by content and context. For example, planning should precede implementation.

This part of ISO/IEC 19770 does not detail documentation in terms of name, format, explicit content and recording media.

Details of certification and recognition schemes are outside of the scope of this part of ISO/IEC 19770.

This part of ISO/IEC 19770 is not intended to be in conflict with any organization's policies, procedures and standards or with any national laws and regulations. Any such conflict should be resolved before using this part of ISO/IEC 19770.