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)

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

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.]

3.35
software asset management
SAM
control and protection of software and related assets within an organization, and control and protection of information about related assets which are needed in order to control and protect software assets

Note 1 to entry: For reference, a corresponding industry definition is "all of the infrastructure and processes necessary for the effective management, control and protection of the software assets within an organization, throughout all stages of their lifecycle".

3.36
software component
entity with discrete structure, such as an assembly or software module, within a system considered at a particular level of analysis

Note 1 to entry: In this part of ISO/IEC 19770, software component refers to a part of a whole, such as a component of a software product, a component of a software identification tag, etc.

3.37
software consumer
entity that uses an *entitlement* (3.14) of a *software package* (3.44)

3.38
software creator
person or organization that creates a *software product* (3.46) or *package* (3.44)

Note 1 to entry: This entity might or might not own the rights to sell or distribute the software.

Note 2 to entry: This part of ISO/IEC 19770 uses the terms software creator and *software licensor* (3.43), rather than common alternatives such as "software publisher" or "software manufacturer", for more precision and hopefully greater clarity.

3.39
software entitlement
software license use rights as defined through agreements between a *software licensor* (3.43) and a *software consumer* (3.37)

Note 1 to entry: Effective use rights take into account any contracts and all applicable licenses, including full licenses, upgrade licenses and maintenance agreements.

3.40
software identification tag
SWID tag
information structure (3.18) containing identification information about a software *configuration item* (3.7), which may be authoritative if provided by a *software creator* (3.38)

3.41
software license
legal rights to use software in accordance with terms and conditions specified by the *software licensor* (3.43)

Note 1 to entry: "Using a software product" can include: accessing, copying, distributing, installing, and executing the software product, depending on the license's terms and conditions.

3.42
software licensee
person or organization granted a license to use a specific software product

3.43
software licensor
person or organization who owns or holds the rights to issue a *software license* (3.41) for a specific software package

Note 1 to entry: This entity might or might not create the software.

Note 2 to entry: This part of ISO/IEC 19770 uses the terms *software creator* (3.38) and software licensor, rather than common alternatives such as "software publisher" or "software manufacturer", for more precision and hopefully greater clarity.

3.44
software package
complete and documented set of *software* (3.34) supplied for a specific application or function

Note 1 to entry: In the ISO/IEC 19770 family of standards, the term software package refers to the set of files associated with a specific set of business functionalities that can be installed on a computing device and has a set of specific licensing requirements. In the ISO/IEC 19770 family of standards, the terms "software product" and "software package" are used synonymously depending on the context of the item described.

3.45
software packager
entity that packages or bundles software created by others

Note 1 to entry: This can be done for example by a value added reseller who bundles a software package to work with an embedded system, or by a software reseller who is licensed to combine a number of different software products into a single bundle.

3.46
software product
complete set of *software* (3.34) designed for delivery to a *software consumer* (3.37) or *end-user* (3.13) that may contain computer programs, procedures, and associated documentation and data

Note 1 to entry: In the ISO/IEC 19770 family of standards, the terms "software product" and "software package" are used interchangeably depending on the context of the item described.

3.47
software usage
consumption against a *software entitlement* (3.39) measured as defined by the terms and conditions of that entitlement

Note 1 to entry: Depending on the specific terms and conditions, usage can include accessing, copying, distributing, installing, and executing software.

3.48
stock keeping unit
sku
identification, usually alphanumeric, of a particular product that allows it to be tracked for inventory and *software entitlement* (3.39) purposes

Note 1 to entry: The term "stock keeping unit" is typically associated with unique products for sales purposes, such as software entitlements. It may not correspond uniquely to specific software products, but may instead represent packages of software, and/or specific terms and conditions related to software products such as whether it relates to a full product, upgrade product, or maintenance on an existing product.

3.49
supplemental {info struct}
{info struct} (3.18) that has a subsidiary relationship to another {info struct}, and extends the information in that {info struct}

3.50
tier
grouping of process definitions

3.51
uniform resource identifier
URI
compact sequence of characters that identifies an abstract or physical resource available on the Internet

Note 1 to entry: The syntax used for URIs shall be as defined in IETF RFC 3986.

[SOURCE: IETF RFC 3986, 1]

3.52
valid
status of an {info struct} that follows the specified *XML Schema document* (3.55) and is valid from an XML perspective

3.53
value baseline
measure of a set of assets before an optimization, assigning relevant values to each group of assets being tracked

3.54
version
unique string of number and letter values indicating a unique revision of an item

Note 1 to entry: Versions are often referred to in software to identify revisions of software that provide unique functionality or fixes. A version typically has multiple parts with at least a major version indicating large changes in functionality or user interface changes and a minor version indicating smaller changes in functionality or user interface changes.

3.55
XML schema document
XSD
document that describes the structure of XML information

[SOURCE: W3C *XML Schema Definition Language (XSD) 1.1 Part 1: Structures*, 1]

4 IT asset management (ITAM) and software asset management (SAM)

4.1 Introduction

Asset management (see 3.3) is a well-established discipline that defines a system consisting of interrelated and interacting parts to establish policies, objectives, strategies, plans and activities to maximize performance and value from a portfolio of assets in the delivery of organizational objectives over a specified period of responsibility. In this context “parts” includes business processes and governance activities, “performance” includes operational, financial and legal performance, and “value” includes minimization of costs and risks.

Asset management is applied at every stage of an asset’s lifecycle. In many industries asset management plays a key role in determining the operational performance and efficiency of an organization.

Information technology (IT) asset management (ITAM) is a sub-discipline of asset management that is specifically aimed at managing the life cycles and total costs of IT assets and the infrastructures that they comprise. ITAM is vital to support life cycle management and strategic decision making for the IT environment, and incorporates specific approaches to handle the portability of some types of IT asset (e.g. laptops and smart phones).

Software asset management (SAM, see 3.35) is a further sub-discipline that is specifically aimed at managing the acquisition, release, deployment, maintenance and eventual retirement of software assets. SAM processes provide effective management, control and protection of software assets within an organization. SAM incorporates specific approaches to handle challenges that are unique to SAM,

such as the real-time mobility of software assets in a distributed and virtualized environment, where such mobility leads to unmanaged growth in number and diversity of software assets.

Although SAM is a sub-discipline of ITAM, for most practical purposes the scope of both is the same, because SAM requires the inclusion in its scope of all other related assets that are necessary to use or manage software in scope. In practical terms this means that all IT hardware assets used for deploying, executing, and managing software must be included in the scope of SAM. Thus the term SAM is used exclusively in the remainder of this clause.

4.2 The need to manage software assets

4.2.1 General

The well-known and inexorable reduction in the cost of computing hardware means that a larger and larger portion of the cost of creating and maintaining an IT infrastructure is related to software assets rather than physical assets. The functionality, complexity and importance of software assets have also markedly increased. Thus it is increasingly important that an organization gains the best value possible for the lifecycle costs of those assets.

Good practice in SAM should result in the types of benefits described in the following subclauses, namely:

a) direct benefits (see 4.2.2);

b) cost control (see 4.2.3); and

c) risk management and mitigation (see 4.2.4).

In addition, certifiable good practice should allow management and other organizations to place reliance on the adequacy of these processes, and the benefits described below should be achieved with a high degree of assurance.

4.2.2 Direct benefits

SAM should provide the following direct benefits:

a) effective deployment of software to the organization supporting the achievement of business objectives;

b) better quality decision making because of more complete and more transparent information availability (for example, IT procurement and system development decisions may be made more quickly and more reliably with better quality data);

c) being able to deploy new systems and functionality more quickly and reliably in response to market opportunities or demands;

d) providing IT which is more closely aligned to business needs, thus ensuring that all users have access to appropriate software and applications;

e) being able to handle the IT aspects of business acquisitions, mergers or demergers more quickly;

f) higher quality IT strategy, enabling the creation of a flexible infrastructure based on modern architectures e.g. cloud-based services and private cloud resiliency; and

g) better personnel motivation and client satisfaction through having less IT problems.

4.2.3 Cost control

SAM should facilitate cost control including in the following areas:

a) reduced direct costs of software and related assets, such as by negotiating better pricing through improved use of volume contracting arrangements, and by avoiding purchasing new licenses when old ones can be redeployed;

b) reduced time and cost for negotiating with suppliers because of better information availability;

c) reduced costs through improved financial control, such as through better invoice reconciliation and more accurate forecasting and budgeting;

d) reduced infrastructure costs for managing software and related assets, by ensuring that required processes are efficient and effective;

e) reduced support costs which are significantly affected by the quality of SAM processes, both directly within IT and indirectly within end-user areas; and

f) better identification of components with the IT infrastructure that incur high costs.

4.2.4 Risk management and mitigation

4.2.4.1 Introduction

SAM should assist in the management and mitigation of risk in a number of areas, as follows:

a) operational (see 4.2.4.2);

b) security (see 4.2.4.3); and

c) compliance (see 4.2.4.4).

4.2.4.2 Operational risk management and mitigation

SAM should facilitate the management of business risks including:

a) risk of interruption to IT services; and

b) risk of deterioration in the quality of IT services

4.2.4.3 Security risk management and mitigation

SAM should help manage and strengthen security through the following:

a) higher assurance about the authorization of installed and/or used software;

b) better identification of non-authorized software; and

c) tighter control of the patch process for installed software.

4.2.4.4 Compliance risk management and mitigation

SAM should promote, and simplify the management, of compliance through minimization of the following:

a) legal and regulatory exposure, especially in regard to personally identifiable information and privacy;

b) license non-compliance;

c) policy non-compliance; and

d) risk of damage to public image arising from any of the above.

4.3 Foundation principles

Software asset management (SAM) as defined in the ISO/IEC 19770 standards is based upon the following principles:

a) That the scope (see 3.32) of the SAM program ultimately includes all types of software (see 3.34) and related assets, regardless of the nature of the software. For example, it can be applied to executable software (such as application programs, operating systems and utility programs), non-executable software (such as fonts, graphics, audio and video recordings, templates, dictionaries, documents and data) and software used other than by installation (such as software as a service and connection-based usage);

b) That the definitions should be applicable to a wide variety of organizations from small to international, to situations where SAM is performed in-house as well as outsourced, and to implementation approaches that range from the highly centralized to completely distributed;

c) That SAM should support a variety of delivery mechanisms (e.g. mobile, premise-based, cloud-based, hosted etc.); and

d) That SAM should support a variety of license models.

The following forms of assets are within the scope of the ISO/IEC 19770 standards:

— **software for use:** all types of software as in a) above;

— **entitlements:** 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); and

— **media:** holding copies of software for use.

4.4 Relationships to principles defined in other standards

4.4.1 Introduction

SAM as defined in the ISO/IEC 19770 family of standards has been defined for consistency with the principles of other ISO standards families, as follows:

a) ISO 9001 (see 4.4.2);

b) ISO/IEC 20000 (see 4.4.3);

c) ISO/IEC 27000 (see 4.4.4); and

d) ISO 55000 (see 4.4.5).

4.4.2 Relationship to ISO 9001 principles

SAM planning and implementation processes as defined in the ISO/IEC 19770 family of standards in principle map to the “Plan-Do-Check-Act” processes of ISO 9001.

4.4.3 Relationship to ISO/IEC 20000 principles

SAM processes as defined in the ISO/IEC 19770 family of standards are closely aligned to and intended to closely support the principles of IT service management as defined in ISO/IEC 20000.

4.4.4 Relationship to ISO/IEC 27000 principles

SAM processes as defined in the ISO/IEC 19770 family of standards are intended to support the security or Integrated Security Management System (ISMS) requirements that are defined or described in ISO/IEC 27000 family.

4.4.5 Relationship to ISO 55000 principles

SAM processes as defined in the ISO/IEC 19770 family of standards should be usable with, and dovetail into, the generic asset management system defined in the ISO 55000 family.

4.5 Principles of process definitions

The ISO/IEC 19770 family of standards contain process definitions in order to be able to codify best practices that form the current state of the art in SAM, and also to facilitate the benchmarking of SAM in different organizations.

However the process definitions (see 3.26) used in the SAM family of standards follow a specific structure in order to be applicable to a wide variety of sizes and types of organization, as follows:

a) The processes are defined in terms of the elements of title, objective, and outcomes. The definitions do not include activities, which are actions that may be used to achieve the outcomes. Those outcomes specified are designed to be readily assessable, but will not necessarily indicate the breadth of activities that may be needed to produce them;

b) The processes are not detailed in terms of methods or procedures required to meet the requirements for outcomes of a process;

c) The sequence of steps an organization should follow to implement SAM is not specified, 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; and

d) Documentation is not detailed in terms of name, format, explicit content and recording media.

NOTE These principles are expected to evolve in future process standards as they are required to meet additional requirements e.g. the requirements for a Management System Standard as defined in Annex SL of the supplement to the ISO/IEC Directives.

4.6 Evaluation of process definition conformance

Conformance to process definitions within the ISO/IEC 19770 family of standards may be performed in one of two ways:

a) By demonstrating that all of the requirements of the process definition have been satisfied using the outcomes as evidence; or

b) By demonstrating that all of the objectives of the process definition have been achieved.

When full conformance is achieved by demonstrating that all of the objectives for a defined tier (see 3.50) have been met, two further requirements exist:

c) Where a process area includes outcomes in different tiers, the objective for that process area shall be interpreted correspondingly for assessments of each tier; and

d) An assessor shall, in addition to reviewing evidence demonstrating that all objectives are achieved, still take into account the specified outcomes for the respective tier. Where there is any failure to meet all specified outcomes, for each such outcome the assessor shall explain in writing their reason(s) for accepting the objectives of a tier are nevertheless still fully satisfied without need for that outcome.

4.7 Principles of information structures

The information structures defined in the ISO/IEC 19770 family of standards adhere to the following principles:

a) The structures are designed to provide interoperability for software management data independent of vendor, platform or technology (such as virtualization);

b) the structures are designed to be usable throughout the software product lifecycle i.e. from the creation stage, through the packaging and installation stages, to the installation, usage, and eventual de-installation stage;

c) the structures are designed to incorporate a unique software_id that corresponds to a unique product at the binary level for distribution/update purposes. Uniqueness is guaranteed by a combination of a unique tag creator name and a tag creator maintained unique_id. A number of different information structures are interlinked by the unique software_id;

d) the structures are designed to minimize the need for a registration authority;

e) the structures are designed to both be readable by humans and interpretable by programs;

f) the structures are designed to be neutral with respect to the platform with which the software assets are associated; and

g) standard locations are defined for each type of platform where the structures are to be located.

4.8 Evaluation of information structure definition conformance

Conformance to definitions of information structures within the ISO/IEC 19770 family of standards may apply to a product or an organization. For organizational conformance, the scope defined shall cover both the organizational scope as well as the products that are included in scope. If an evaluation is made of a product or organization, the evaluation shall specify the scope for which conformance was tested.

There are a number of reasons for an organization to evaluate individual product conformance against the ISO/IEC 19770 family of standards. This may be sought when a specific product is being provided for a market that requires conformance (for example, if government organizations require products to follow the ISO/IEC 19770 family of standards in order to be included on a project). It may also be desired by platform providers who want to provide a more secure and auditable ISO/IEC 19770 information structures that can be used to support definitive processes e.g. to clearly identify which end-users installed which software packages.

Organizations may want to adhere to the ISO/IEC 19770 family of standards for a number of reasons. For example, software providers may want to promote their software products as being easier to manage. Also, software consumers may want to show that they are actively managing their software assets and may desire to demonstrate that they can provide accurate information to any reconciliation or audit request.

4.9 Critical success factors

The critical success factors for any SAM program are:

a) a clear sense of direction and ownership for the program from executive management;

b) a clear definition of scope (either organizational or product) and roles and responsibilities relevant to the program; and

c) a clear understanding of the software use rights that apply to all of the software assets being managed.

5 ITAM family of standards

5.1 General information

The ISO/IEC 19770 family of standards includes standards that:

a) define processes (see 3.26) that enable an organization to demonstrate that it is performing software asset management (SAM) to a level sufficient to satisfy corporate governance requirements and ensure effective control and protection of software (see 3.34) assets within an organization;

b) define an approach to the implementation of the processes in a) above that consists of a number of defined tiers (see 3.50) that can be achieved, with appropriate recognition of conformance;

c) define information structures (see 3.18) that support the processes in a) above and contain authoritative identification and management information about a software product; and

d) define additional information structures associated with specific asset management functions e.g. entitlement (see 3.14), that can supplement the information contained in the foundation information structures in c) above.

The ISO/IEC 19770 family of standards are illustrated in Figure 1 below:

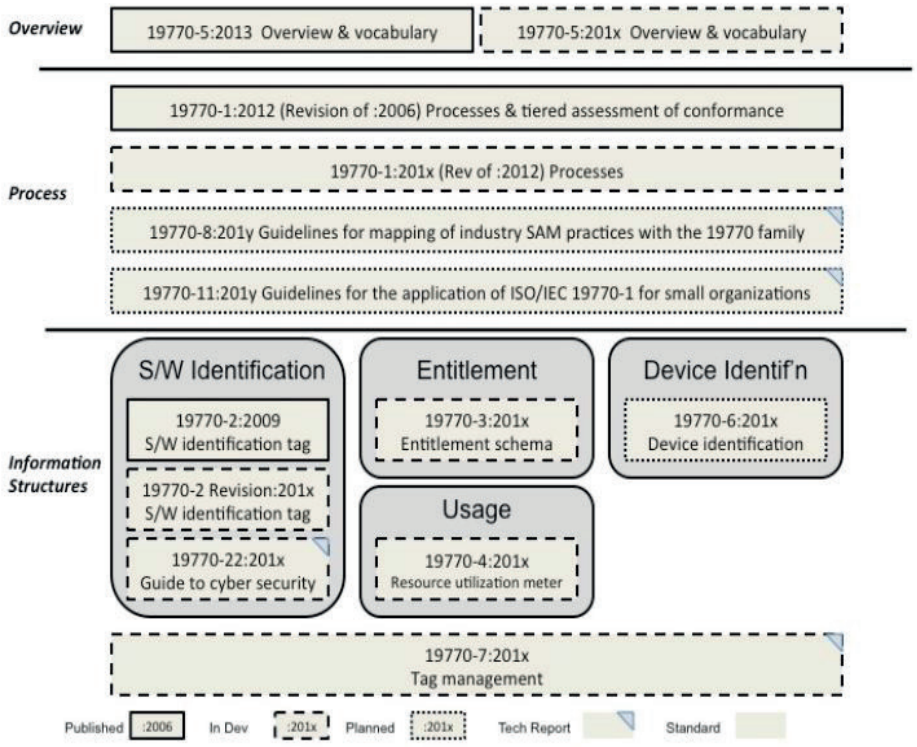

Figure 1 — ISO/IEC 19770 family of standards functional block diagram

5.2 Standards specifying processes

5.2.1 ISO/IEC 19770-1:2006

Information technology — Software asset management — Part 1: Processes

Note This original 2006 version of ISO/IEC 19770-1 has been superseded by the 2012 version (see 5.2.2).

Scope: This part of ISO/IEC 19770 establishes a baseline for an integrated set of processes (see 3.26) for SAM.

Purpose: ISO/IEC 19770-1 describes SAM processes that can be implemented by organizations to achieve immediate benefits. It is intended that ISO/IEC 19770-1 be an implementation standard for organizations. ISO/IEC 19770-1 applies to all organizations of any size or sector but can only be applied to a legal entity, or to parts of a single legal entity.

5.2.2 ISO/IEC 19770-1:2012

Information technology — Software asset management — Part 1: Processes and tiered assessment of conformance

Scope: This part of ISO/IEC 19770 establishes a baseline for an integrated set of processes for SAM, divided into tiers (see 3.50) to allow for implementing them, and achieving recognition, incrementally.

Purpose: The "second generation" ISO/IEC 19770-1:2012 was directed by feedback on the "first generation" standard ISO/IEC 19770-1:2006, which is a comprehensive standard designed to align with all of service management as specified in ISO/IEC 20000. However, market feedback was received that organizations wanted something that could be accomplished in stages. This part of ISO/IEC 19770 has been designed to make this possible, calling these stages "tiers". The first three tiers consist of selected subsets of the total set of process areas and outcomes maintaining the same structure and approach as for ISO/IEC 19770-1:2006. Accomplishing the fourth and final tier of this part of ISO/IEC 19770 is essentially identical to conformance with ISO/IEC 19770-1:2006.

5.2.3 ISO/IEC 19770-1:201x

Information technology — IT asset management — Part 1: IT asset management systems — Requirements

Scope: This part of ISO/IEC 19770 specifies the requirements for the establishment, implementation, maintenance and improvement of a management system for IT asset management, referred to as an "IT asset management system".

Purpose: The "third generation" of ISO/IEC 19770-1 (currently in development) is a revision of ISO/IEC 19770-1:2012 to comply with the High Level Structure and Common Wording as now required by ISO for all Management System Standards. It includes all normative text from ISO 55001 for (generic) asset management, and adds requirements specific to IT assets, and software in particular.

5.3 Technical reports providing guidance for process standards

5.3.1 ISO/IEC 19770-8:201x

Information technology — Software asset management — Part 8: Guidelines for mapping of industry SAM practices with the ISO/IEC 19770 *family of standards*

Scope: This part of ISO/IEC 19770 identifies correspondences and differences between the definitions contained in the ISO/IEC 19770 family of standards and existing industry practices.

Purpose: ISO/IEC 19770-8 builds on the cross-reference to industry best practice guidance given in Annex C of ISO/IEC 19770-1:2012 (see 5.2.2). There has been strong support for including such information in ISO/IEC 19770-1:2012, but at the same time WG21 has recognized the ongoing maintenance issues of including this information in a published standard that is revised on a different timetable than that of the source documents. Thus WG21 intends to formally request each subject-matter owner to consider providing text for inclusion in this technical report, and to request that frequent updates are issued. The availability of these mappings is expected to accelerate the enhancement of industry standard approaches to conform to the full requirements of the ISO/IEC 19770 family.

5.3.2 ISO/IEC 19770-11:201x

Information technology — Software asset management — Part 11: Guidelines for the application of ISO/IEC 19770-1 *for small organizations*

Scope: This part of ISO/IEC 19770 gives specific guidance on applying the processes for SAM to small organizations, with specific reference to the tiers defined in ISO/IEC 19770-1:2012.

Purpose: ISO/IEC 19770-11 provides detailed guidance on implementing Software asset management in small organizations, including simplified governance and management structures, modified process definitions, and redefinitions of roles appropriate to manual procedures performed by a small number of people.

5.4 Standards specifying information structures

5.4.1 ISO/IEC 19770-2:2009

Information technology — Software asset management — Part 2: Software identification tag

Scope: This part of ISO/IEC 19770 establishes specifications for tagging software to optimize its identification and management.

Purpose: ISO/IEC 19770-2 provides a standard for software identification tags (see 3.40). The software identification tag is an XML file containing authoritative identification and management information about a software product. The software identification tag is installed and managed on a computing device together with the software product. The tag may be created as part of the installation process, or added later for software already installed without tags. However, it is expected more commonly that the tag will be created when the software product is originally developed, and then be distributed and installed together with the software product. Having the tag available from the beginning allows for the more effective management of distribution and repackaging external to the software consumer, and then of release management within the software consumers organization.

5.4.2 ISO/IEC 19770-2:201x

Information technology — Software asset management — Part 2: Software identification tag

Scope: This part of ISO/IEC 19770 addresses structural extensions to the ISO/IEC 19770-2:2009 to facilitate greater market adoption, and to promote more semantic interoperability between producers of tags and consumers of tags.

Purpose: ISO/IEC 19770-2 provides improvements to ISO/IEC 19770-2:2009 resulting from market feedback and deployment experience. Four of the top eight independent software vendors identified in the Forbes Global 2000 now distribute software identification tags with their products, and many millions of such tags are found in the field. There are also tool providers creating software identification tags (installation tools) or reading and using software tags (discovery & compliance tools). All of this deployment has generated a significant amount of high-quality feedback identifying defects in ISO/IEC 19770-2:2009 and suggesting improvements, clarifications, and extensions. Much of this feedback has been received via a not-for-profit organization named TagVault.org (www.tagvault.org) that has also been formed to promote software identification tags, and vhich is a Class C Liaison organization to WG21.

5.4.3 ISO/IEC 19770-3:201x

Information technology — IT asset management — Part 3: Entitlement schema

Scope: This part of ISO/IEC 19770 establishes specifications for unambiguous definition of software entitlements to effectively demonstrate ownership of entitlements, optimize reconciliation of installed software with entitlements, demonstrate compliance, and optimize licensing for cost reduction.

Purpose: ISO/IEC 19770-3 provides for unambiguous definition of entitlements. The entitlement schema provides authoritative licensing information for software configuration items specified in ISO/IEC 19770-2:2009. Standardization of entitlements provides uniform, measurable data for the license compliance processes of SAM practice, making optimization of the reconciliation of software with licensing entitlements possible.

5.4.4 ISO/IEC 19770-4:201x

Information technology — IT asset management — Part 4: Resource utilization measurement

Scope: This part of ISO/IEC 19770 establishes specifications for a format to contain information related to the usage of the software assets and their related resources. This definition will be created in a manner that is consistent with the identification information defined in 19770-2, and with the entitlement information defined in 19770-3, and when used together these three types of information have the capability to significantly enhance and automate the processes of IT asset management.

Purpose: ISO/IEC 19770-4 provides a standard for resource utilization measurement information (RUM) structures. The RUM incorporates a standardized structure containing authoritative usage information about consumption of resources related to the use of a software asset. The structure will be created in a manner that is consistent with the identification information defined in ISO/IEC 19770-2, and with the entitlement information defined in ISO/IEC 19770-3, and when used together these three types of information have the capability to significantly enhance and automate the processes of IT asset management.

5.4.5 ISO/IEC 19770-6:201x

Information technology — Software asset management — Part 6: Device Identification

Scope: This part of ISO/IEC 19770 provides specifications for the identification and management of devices containing embedded software.

Purpose: ISO/IEC 19770-6 describes the use of the information structures defined by other parts of ISO/IEC 19770 in devices containing embedded software.

5.5 Technical reports providing guidance for information structure standards

5.5.1 ISO/IEC 19770-7:201x

Information technology — Software asset management — Part 7: Tag management

Scope: This part of ISO/IEC 19770 provides a baseline for the practices associated with the management of all software tags defined by the ISO/IEC 19770 family of standards.

Purpose: ISO/IEC 19770-7 describes a cohesive roadmap and guidance that can be used for ongoing management of information structures defined by the ISO/IEC 19770 family of standards. A need has been identified for market guidance on how software identification tags, and software entitlement tags should be managed individually, with each other, and with other data needed for overall software management.

5.5.2 ISO/IEC 19770-22:201x

Information technology — Software asset management — Part 22: Guidance for the use of 19770-2 Software Identification Tag information in Cyber Security

Scope: This part of ISO/IEC 19770 provides definitions of how the contents of the information structures defined by other parts of ISO/IEC 19770 may be utilized for the purposes of cyber security. However most of the information being considered is defined in ISO/IEC 19770-2, software identification tag.

Purpose: ISO/IEC 19770-22 describes a number of potential uses for uses for the tag information that have been discovered, including ISO/IEC 29147 and ISO/IEC 3011 related vulnerability disclosure and vulnerability handling process, ISO/IEC 27001 controls related to system integrity, specific processes in the ISO/IEC 27034 multi-part standard related to provisioning applications and auditing their security, and definitions in ISO/IEC 27036 related to ensuring the integrity of IT products and services.

5.6 Overview standards

5.6.1 ISO/IEC 19770-5:2013

Information technology — Software asset management — Part 5: Overview and vocabulary

Scope: This part of ISO/IEC 19770 provides an overview of the ISO/IEC 19770 family of standards, an introduction to SAM, a brief description of the foundation principles and approaches on which SAM is based; and consistent terms and definitions for use throughout the ISO/IEC 19770 family of standards.

Purpose: ISO/IEC 19770-5 describes the fundamentals of software asset management (SAM), gives an overview of the ISO/IEC 19770 family of standards, and defines terminology for use throughout that family of standards.

5.6.2 ISO/IEC 19770-5:2015 (this standard)

Information technology — Software asset management — Part 5: Overview and vocabulary

Scope: This part of ISO/IEC 19770 provides enhancements to the overview of the ISO/IEC 19770 family of standards, and the common vocabulary for use throughout that standards family, that was contained in ISO/IEC 19770-5:2013.

Purpose: ISO/IEC 19770-5 describes an overview of the ISO/IEC 19770 family of standards that is consistent with Revision 9.3 of the WG21 Strategic Plan that was approved in Sydney in June 2014, and updates terminology for use throughout that family of standards in line with developments since 2011.

Bibliography

[1] ISO/IEC/IEEE 24765:2010[2], *Systems and software engineering — Vocabulary*

[2] Extensible Markup Language (XML) 1.1 (Second Edition), W3C Recommendation, http://www.w3.org/TR/2008/REC-xml-20081126/

[3] XML Schema Definition Language (XSD) 1.1 Part 1: Structures, W3C Recommendation, http://www.w3.org/TR/xmlschema11-1/

[4] XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes, W3C Recommendation, http://www.w3.org/TR/xmlschema11-2/

[5] RFC 1034, *Domain Names — Concepts and Facilities*, November 1987, http://tools.ietf.org/html/rfc1034

2) ISO/IEC/IEEE 24765 is a "snapshot" of the SEVOCAB (systems and software engineering vocabulary) database, which is available at: http://www.computer.org/sevocab

ICS 35.080

Price based on 19 pages