BS ISO/IEC 19770-1:2012

BSI Standards Publication

Information technology — Software asset management

Part 1: Processes and tiered assessment of conformance

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 19770-1:2012

National foreword

This British Standard is the UK implementation of ISO/IEC 19770-1:2012. It supersedes BS ISO/IEC 19770-1:2006, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/15, Software and systems engineering.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2012.
Published by BSI Standards Limited 2012.

ISBN 978 0 580 71806 9

ICS 35.080

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2012.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19770-1:2012

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)

Documents
Document Sharing Hub
© ISO/IEC 2012

Full document details: BS ISO/IEC 19770-1:2012

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19770-1:2012

Contents

Page

Foreword iv

Introduction v

1 Scope 1
1.1 Purpose 1
1.2 Field of application 1
1.3 Limitations 3

2 Conformance 3
2.1 Intended usage 3
2.2 Methods of demonstrating full conformance 3

3 Terms and definitions 4

4 SAM processes 6
4.1 General 6
4.2 Control environment for SAM 8
4.3 Planning and implementation processes for SAM 12
4.4 Inventory processes for SAM 16
4.5 Verification and compliance processes for SAM 19
4.6 Operations management processes and interfaces for SAM 23
4.7 Life cycle process interfaces for SAM 27

5 Tiers 33
5.1 Overview 33
5.2 Tier 1 – trustworthy data 35
5.3 Tier 2 – practical management 36
5.4 Tier 3 – operational integration 37
5.5 Tier 4 – full ISO/IEC SAM conformance 38

Annex A (informative) **Reference chart of outcomes by tier** 39

Annex B (informative) **Guidance on selected topics** 43

Annex C (informative) **Cross reference to industry best practice guidance** 45

Annex D (informative) **Roadmap** 73

Annex E (informative) **Industry capability/maturity approaches** 75

Bibliography 80

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

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.

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

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:

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

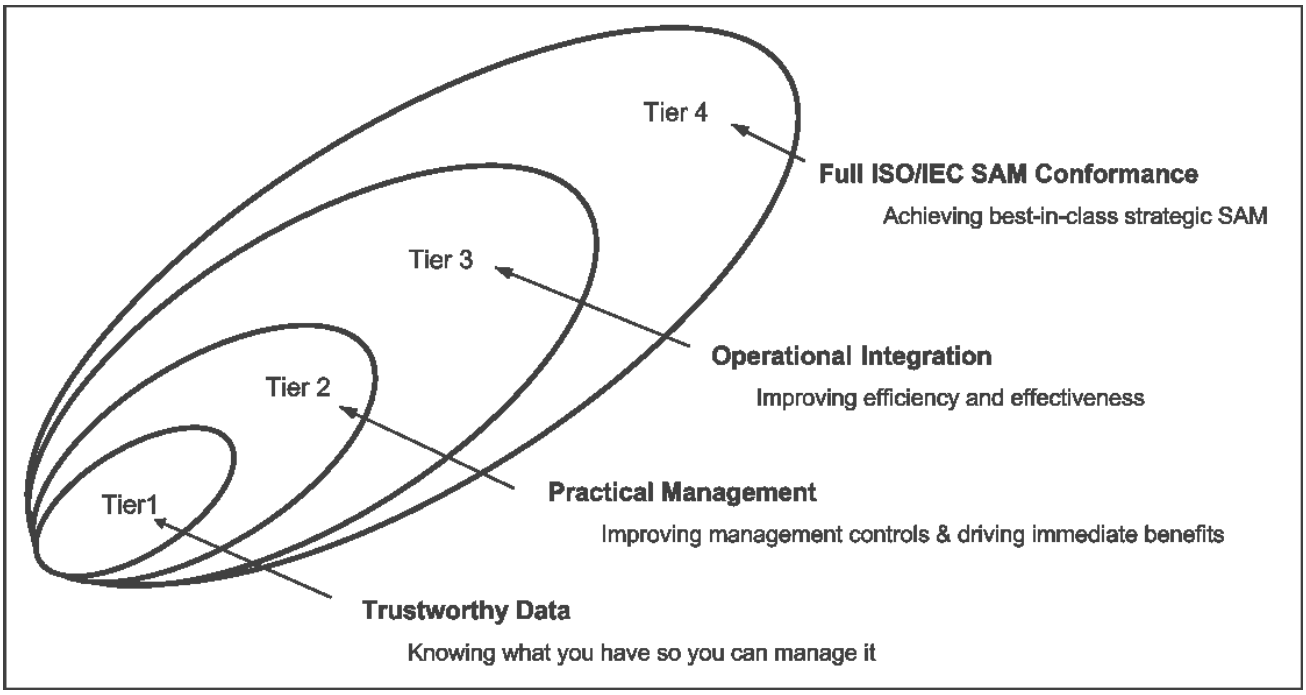

Figure 1 — The four tiers of SAM

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.

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

- 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.

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19770-1:2012

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*.

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 19770-1:2012

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

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

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.

2 Conformance

2.1 Intended usage

This part of ISO/IEC 19770 is intended for use as best practice guidance, and also to allow for the possibility of independent certification of achievement of the individual tiers. There is choice, however, in the ways of assessing an organization's conformance.

This part of ISO/IEC 19770 has been written to allow continuity with ISO/IEC 19770-1:2006, but in addition to allow assessment following the same approach used in other standards that are accepted as defining a management system standards framework as defined in ISO Guide 72. In particular, this means that the assessor has the newly added option of assessing against the overall objective of each of the process areas, or the previous approach of assessing against all of the detailed outcomes for each of the process areas, as for ISO/IEC 19770-1:2006. One choice must be applied consistently as a way of assessing across all process areas.

2.2 Methods of demonstrating full conformance

The requirements in this part of ISO/IEC 19770 are contained in the objectives and outcomes listed within Clause 4 of this part of ISO/IEC 19770. Any claim of conformance shall be a claim of full conformance to the provisions of this part of ISO/IEC 19770 as described below, including for any outsourced processes.

Full conformance with any of the tiers of this part of ISO/IEC 19770 is achieved in either of two ways:

- By demonstrating that all of the requirements of the respective tier of this part of ISO/IEC 19770 have been satisfied using the outcomes as evidence; or

- By demonstrating that all of the objectives of the respective tier of this part of ISO/IEC 19770 have been achieved.

Furthermore, it must be demonstrated that any underlying tiers are currently certified for full conformance and that they are being monitored for continuing full conformance by a surveillance program accepted by the assessor; or alternatively that any underlying tiers are being certified as part of the current assessment.

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

If full conformance is achieved by demonstrating that all of the objectives of the respective tier of this part of ISO/IEC 19770 have been met, two further requirements exist:

- Where a process area includes outcomes in different tiers, the objective for that process area shall be interpreted correspondingly for assessments of each tier.

- The 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.

For the avoidance of doubt, where outcomes are specified using the word “including” which is then followed by a list, this is to be understood as requiring all of the items in the list, with additional unlisted items possible but not required.

3 Terms and definitions

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

3.1
baseline
snapshot of the state of a service or individual configuration items (3.2) at a point in time

[ISO/IEC 20000-1:2005]

3.2
configuration item
CI
component of an infrastructure or an item which is or will be under control

NOTE 1 For the purpose of this part of ISO/IEC 19770, 'under control' means under the control of inventory processes. Inventory processes for SAM (4.4) are the basis not only for SAM, but for all of configuration management.

NOTE 2 Configuration items or CIs are commonly defined as part of Service Management practice and 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.

3.3
corporate board or equivalent body
person or group of people who assumes legal responsibility for conducting or controlling an organization at the highest level

3.4
definitive master version
originating instance of the software that is used to install or provision the software

EXAMPLE Source used to create distribution copies.

NOTE *Install* can apply to executable or non-executable software, or related assets such as fonts. It can apply to installs on clients/local devices and/or server-side installs, for example as part of a service-type software asset provision.

3.5
distribution copy
copy of the software definitive master version, for the purposes of installation onto other hardware, which resides for example on a server, or on physical media such as CDs

3.6
effective full license
license rights for software which allow one full use of the software

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

NOTE 1 An effective license consists of one or more underlying licenses (3.16).

EXAMPLE In some licensing an underlying full license for version 1 of a software product, plus an underlying upgrade license to version 2 of the software product, combine to produce one effective full license for version 2 of the software product. In this example, sometimes the upgrade license rights can come from a support contract or subscription.

NOTE 2 Full use of the software is as defined in the terms and conditions of the license(s).

3.7
local SAM owner
individual at any level of the organization below that of the SAM owner (3.13) who is identified as being responsible for SAM for a defined part of the organization.

3.8
personnel
any individual expected to perform duties on behalf of the organization, including officers, employees and contractors

3.9
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 A platform is distinct from the unique instances of that platform, which are typically referred to as devices or instances.

3.10
procedure
specified way to carry out an activity or process

NOTE 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 (3.11).

3.11
process
set of interrelated activities, which transforms inputs into outputs

NOTE 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 (3.10).

3.12
release
collection of new and/or changed configuration items which are tested and introduced into a live environment together

NOTE A release must have technical approval for this purpose but may not yet be authorized for deployment. A release may consist of source-code, code for execution or of multiple software assets packaged into an internal production release and tested for a target platform.

[ISO/IEC 20000-1:2005, with note added specific to this part of ISO/IEC 19770.]

3.13
SAM owner
individual at a senior organization-wide level who is identified as being responsible for SAM

3.14
software
all or part of the programs, procedures, rules, and associated documentation of an information processing system

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

NOTE 1 There are multiple definitions of software in use. For the purpose 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, and documents. (See also 1.2 Field of Application.)

NOTE 2 The user of this part of ISO/IEC 19770 is required to define their own scope for its application, and may restrict the types of software to be considered in scope. (See also Clause 1 Scope.)

[ISO/IEC 2382-1:1993, 01.01.08, with notes added specific to this part of ISO/IEC 19770.]

3.15
software asset management
SAM
effective management, control and protection of software assets within an organization, and the effective management, control and protection of information about related assets which are needed in order to manage software assets.

NOTE A corresponding definition from the Information Technology Infrastructure Library (ITIL®) 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"

3.16
underlying license
license for software use as originally purchased or procured, and which can typically be linked directly to purchase records

NOTE An underlying license may have conditions associated with it, requiring it to be used in combination with another license or licenses to create an effective full license (3.6). It may also have capacity or permission to use future versions of the software, or specify ways or limitations to how it may be upgraded or replaced by a new version, or how the license may be upgraded by combining with another license that is linked directly to a another purchase record.

4 SAM processes

4.1 General

4.1.1 Definition and relationship to service management

Software asset management is the effective management, control and protection of software assets within an organization, and the effective management, control and protection of information about related assets which are needed in order to manage software assets.

SAM processes as defined in this part of ISO/IEC 19770 are closely aligned to and intended to closely support IT service management as defined in ISO/IEC 20000-1.

4.1.2 Overview of SAM processes

The overall conceptual framework for SAM processes is comprehensive and does not by itself reflect the Tiers as described in the Introduction or in Clause *5 Tiers*. Figure 1 below gives the conceptual framework for the SAM processes and is broken down into three main categories:

a) Organizational management processes for SAM;

b) Core SAM processes;

c) Primary process interfaces for SAM.

The processes are described in further detail in 4.2 to 4.7.

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

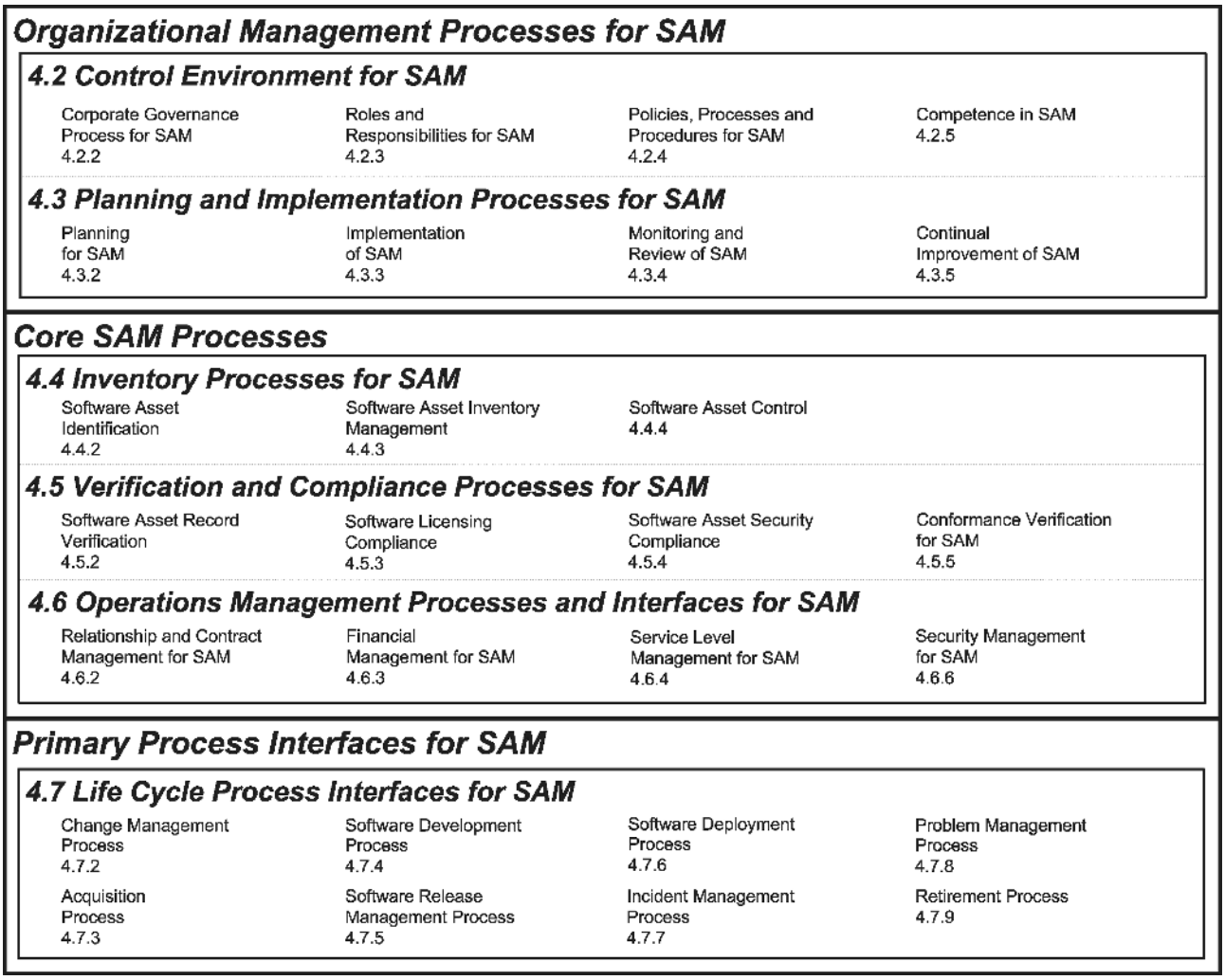

Figure 2 — Framework for SAM processes

4.1.3 Outcomes, activities and interfaces

This part of ISO/IEC 19770 has been written using the process elements of title, objective, and outcomes. This part of ISO/IEC 19770 does not include activities, which are actions which may be used to achieve the outcomes.

The outcomes specified in this part of ISO/IEC 19770 are designed to be readily assessable, but will not necessarily indicate the breadth of activities which may be needed to produce them. For example, the maintenance of inventories in the *Software asset inventory management* process will logically require data validation activities, although this is not cited as an outcome in this part of ISO/IEC 19770. (Data integrity is assured in this part of ISO/IEC 19770 by the *Verification and compliance processes for SAM*.)

Some of the most important activities are interface activities with other processes. For example, when a software asset is purchased (or 'acquired') the objective to be met is "The objective of the *Acquisition process* in respect of software and related assets is to ensure that they are acquired in a controlled manner and recorded." This process, and many others, will require an invoking of the *Software asset inventory management* process to record the data and validate it for required fields etc. Another example is the creation of baselines, which are created in the *Software asset control* process. This process is invoked by the *Software development process* and the *Software release management process*. It is not the objective of this part of ISO/IEC 19770 to specify this type of detail, but such activities or interfaces are implicitly required in order to achieve the stated objectives.

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

4.2 Control environment for SAM

4.2.1 General

The *Control environment for SAM* establishes and maintains the management system within which the other SAM processes are implemented.

The *Control environment for SAM* consists of the following process areas:

a) *Corporate governance process for SAM*;

b) *Roles and responsibilities for SAM*;

c) *Policies, processes and procedures for SAM*;

d) *Competence in SAM*.

4.2.2 Corporate governance process for SAM

4.2.2.1 Objective

The objective of the *Corporate governance process for SAM* is to ensure that responsibility for management of software assets is recognized at the level of the corporate board or equivalent body, and that appropriate mechanisms are in place to ensure the proper discharge of this responsibility. NOTE This process could be considered part of overall corporate governance of IT – see ISO/IEC 38500.	Applicable to tiers 2 and 4

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

4.2.2.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Corporate governance process for SAM* will enable the organization to demonstrate that:				
a) There is a clear corporate statement of organizational scope for the purposes of this part of ISO/IEC 19770 about:		•		
1) the legal entity or parts of a legal entity which are included in scope. NOTE One factor to consider in defining organizational scope may be existing software contracts which are based on specific organizational scopes.				
2) the specific single body or individual that has overall corporate management responsibility for that entity or parts of that entity. NOTE This specific body or individual is referred to subsequently as the 'corporate board or equivalent body'.				
b) Responsibility for corporate governance of software and related assets is formally recognized by the corporate board or equivalent body.		•		
c) Corporate governance regulations or guidelines which are relevant to the organization for its use of software and related assets, in all countries where it operates, have been identified and documented, and are reviewed at least annually.		•		
d) An assessment of the risks associated with software and related assets, and management-specified mitigation approaches, is documented, updated at least annually, and approved by the corporate board or equivalent body, covering at least the following:		•		
1) Risk of regulatory non-compliance. NOTE This could refer for example to privacy protection for personnel software usage monitoring; data protection for SAM records held on individuals; and industry-specific requirements, such as in the pharmaceutical industry.				
2) Risk of violation of security requirements. NOTE The impact of security violations may include for example the interruption of business operations, the misuse of confidential information by competitors, and reputational damage resulting from insufficient protection of customer privacy.				
3) Risk of licensing non-compliance.				
4) Risk of interruption of operations due to problems with the IT infrastructure which could result from inadequate SAM.				
5) Risk of excessive spending on licensing and other IT support costs due to inadequate SAM.				
6) Risks associated with decentralized vs. centralized management approaches for software and related assets. NOTE It may be highly desirable for culture and efficiency reasons to decentralize operational management of SAM. However, such approaches may find it more difficult to achieve cost savings, and may have higher risk exposures, such as to licensing non-compliance, than centralized management approaches. For example, any licensing non-compliance in any decentralized operation still threatens the reputation and creates legal exposure for the entire organization. It is probably prudent, even in a decentralized operational management environment, to centrally manage selected information and management review in such a way that distributed management can operate SAM without increased risk. Managing centralized information itself usually involves some centralized management oversight for SAM.				
7) Risks associated with different countries of operation taking into account local compliance cultures and enforcement approaches.				
e) The management objectives for SAM are approved by the corporate board or equivalent body, and reviewed at least annually.				•

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

4.2.3 Roles and responsibilities for SAM

4.2.3.1 Objective

The objective of the *Roles and responsibilities for SAM* process is to ensure that the roles and responsibilities for software and related assets are clearly defined, maintained and understood by all personnel potentially affected. NOTE These roles and responsibilities include in particular any which link into regulatory or corporate governance requirements.	Applicable to Tier 2

4.2.3.2 Outcomes

Outcome	Tier			
	1	2	3	4
Implementation of the *Roles and responsibilities for SAM* process will enable the organization to demonstrate that:				
a) The role of the SAM owner, responsible for corporate governance of software and related assets for the entire organization, is clearly defined and approved by the corporate board or equivalent body. Responsibilities assigned include the following for the entire organization:		•		
1) Proposing management objectives for SAM.				
2) Overseeing the development of the SAM plan.				
3) Obtaining resources for implementing the approved SAM plan.				
4) Delivering results against the approved SAM plan.				
5) Ensuring that all local SAM owners discharge their responsibilities properly, and that all parts of the organization are covered by the SAM owner or local SAM owners, without conflicting overlap.				
b) Local roles and responsibilities for corporate governance of software and related assets are documented and assigned to specified individuals. Responsibilities assigned include the following for the part of the organization for which each individual is responsible:		•		
1) Obtaining resources for implementing the approved SAM plan.				
2) Delivering results against the approved SAM plan.				
3) Adopting and implementing necessary policies, processes and procedures.				
4) Maintaining accurate records of software and related assets.				
5) Ensuring that management and technical approvals are required for procurement, deployment and control of software assets.				
6) Managing contracts, supplier relationships, and internal customer relationships.				
7) Identifying the need for and implementing improvements.				
NOTE 1 This part of ISO/IEC 19770 differentiates between the corporate SAM owner and local roles and responsibilities because some organizations with multiple locations make such a distinction in their management roles. Where there is only one location, or the remote locations are small and directly managed by the central location, then these two sets of functions merge. NOTE 2 Responsibilities may be assigned to specific positions, or to classes of positions, so long as the nature of those responsibilities, and accountability for their discharge, is clear. In practice, this means that it is not necessary to assign different responsibilities to different physical persons, especially in smaller organizations where such division of duties is not practical.				
c) These responsibilities are communicated to all parts of the organization involved in any way with SAM, in the same way as other organization-wide and local policies are communicated.		•		

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

4.2.4 Policies, processes and procedures for SAM

4.2.4.1 Objective:

The objective of the *Policies, processes and procedures for SAM* process is to ensure that an organization maintains clear policies, processes and procedures to ensure effective planning, operation and control of SAM.	Applicable to Tier 2

4.2.4.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Policies, processes and procedures for SAM* process will enable the organization to demonstrate that:				
a) There is a structured approach to creating, reviewing, approving, issuing, and controlling policies, processes, procedures and related documentation relevant to SAM so that it is always possible to determine the complete set available, which version of each document is currently in effect and which documents apply to different types of software and related assets. NOTE This would typically be part of an overall approach adopted by an organization for all of its policies, processes and procedures, and not be unique for SAM.		•		
b) Policy, process and procedure documentation required by this part of ISO/IEC 19770 are organized by the process classifications of this part of ISO/IEC 19770 or with a cross-reference to these classifications.		•		
c) Policies are developed, approved and issued covering at a minimum:		•		
1) Individual and corporate responsibilities for corporate governance of software and related assets.				
2) Any restrictions on personal use of corporate software and related assets.				
3) Requirement for compliance with legal and regulatory requirements, including for copyright and data protection.				
4) Any procurement requirements (e.g. use of corporate agreements, or buying only from reputable/approved suppliers)				
5) Any requirement for approvals for installation or use of software, whether purchased or not.				
6) Disciplinary implications of violation of these policies.				
NOTE The policies above are to cover generic requirements, including for end-users in particular. Policies and procedures relevant for specific process areas are covered in the appropriate process areas.				
d) Policies and procedures are communicated to all personnel in a way which (1) reaches all new personnel when they start, and continuing personnel at least annually; (2) requires positive acknowledgement back from personnel when they start and at least annually; and (3) is readily accessible at all times to personnel. NOTE The documentation can be in any form or medium. The documentation may be issued in consolidated versions with other documents, such as consolidated policy statements covering also personnel confidentiality requirements.		•		

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

4.2.5 Competence in SAM

4.2.5.1 Objective

The objective of the *Competence in SAM* process is to ensure that appropriate competence and expertise in SAM is available and is being applied.	Applicable to tiers 2 and 4

4.2.5.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Competence in SAM* process will enable the organization to demonstrate that:				
a) A review is documented and updated at least annually which covers the availability and uptake of training and certification by personnel with SAM responsibilities for:		●		
1) SAM in general.				
2) Licensing for software manufacturers whose software is being used. NOTE Software covered by this requirement is only that software defined as being in scope (see 4.2.2.2.a1 and 4.3.2.2.b1)				
b) A review is undertaken at least annually to determine what constitutes "Proof of License" for the software manufacturer.				●
c) Personnel with SAM management responsibilities receive training in SAM and in relevant licensing, including both initial training and formal continuing education annually. NOTE Individual qualifications are also recommended, to the extent available.		●		
d) A review is undertaken at least annually to ascertain what, if any, extra guidance is offered by the software manufacturers to enable compliance with their licenses.		●		

4.3 Planning and implementation processes for SAM

4.3.1 General

The *Planning and implementation processes for SAM* ensure the effective and efficient accomplishment of SAM management objectives.

The processes in this area map, in principle, to the 'Plan-Do-Check-Act' processes of ISO/IEC 9001.

Planning and implementation processes for SAM consists of the following process areas:

a) *Planning for SAM*;

b) *Implementation of SAM*;

c) *Monitoring and review of SAM*;

d) *Continual improvement of SAM*.

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

4.3.2 Planning for SAM

4.3.2.1 Objective

The objective of the *Planning for SAM* process is to ensure appropriate preparation and planning for the effective and efficient accomplishment of SAM objectives.	Applicable to tiers 2 and 4

4.3.2.2 Outcomes

Outcome	Tier			
	1	2	3	4
Implementation of the *Planning for SAM* process will enable the organization to demonstrate that:				
a) Management objectives for SAM are developed and proposed for approval by the corporate board or equivalent body, and updated at least annually.				●
b) A plan (the 'SAM plan') for implementing and delivering SAM is developed and documented, and updated at least annually, which includes:		●		
1) A clear scope statement (an unambiguous 'software asset scope') describing which types of software are included; the coverage of software and related assets, shall be stated e.g. percent inventory completeness for last SAM Plan update, giving actual and plan figures; any coverage of assets beyond the minimum required by this part of ISO/IEC 19770; and any interfaces with or requirements for other organizations or systems. See also organizational scope: 4.2.2.2.a1.				
2) A clear specification of which policies, processes and procedures are required for assets in scope.				
3) A clear explanation of the approach to managing, auditing and improving SAM including automation as appropriate to support the processes.				
4) An explanation of the approach to be used to identifying, assessing and managing issues and risks related to the achievement of the defined management objectives.				
5) Schedules and responsibilities for periodic activities, including preparation of management reports and performance of verification and compliance activities.				
6) Identification of the resources including budget needed to implement the SAM plan.				
7) Performance measures for tracking accomplishment against the SAM plan, including target measures for accuracy of the asset management records.				
NOTE An appropriate level of automation should be implemented and included in the SAM plan to ensure that processes do not become inefficient or error prone, or may not be followed at all.				
c) The plan is approved by the corporate board or equivalent body.		●		

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

4.3.3 Implementation of SAM

4.3.3.1 Objective

The objective of the *Implementation of SAM* process is to accomplish overall SAM objectives and the SAM plan.	Applicable to Tier 4

4.3.3.2 Outcomes

Outcome	Tier			
	1	2	3	4
Implementation of the *Implementation of SAM* process will enable the organization to demonstrate that:				
a) Mechanisms are in place to collect information, including from local SAM owners, about changes, issues and risks that affect the SAM plan throughout the year.				•
b) Regular status reports (at least quarterly) are prepared by the SAM owner detailing the overall progress against the SAM plan for reporting to the corporate board or equivalent body.				•
c) Follow-up on any variances identified takes place promptly and is documented.				•

4.3.4 Monitoring and review of SAM

4.3.4.1 Objective

The objective of the *Monitoring and review of SAM* process is to ensure that the management objectives for SAM are being achieved.	Applicable to tiers 2 and 4

4.3.4.2 Outcomes

Outcome	Tier			
	1	2	3	4
Implementation of the *Monitoring and review of SAM* process will enable the organization to demonstrate that:				
a) A formal review is conducted at least annually:				•
1) to assess whether management objectives for SAM and the SAM plan are being achieved				
2) to summarize performance against all performance measures specified in the SAM plan and in service level agreements related to SAM NOTE Service Level Agreements covering requirements for SAM could cover more than just SAM.				
3) to provide a summary of the findings of the *Conformance verification for SAM* process				

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
4) to conclude on the basis of the above whether:				
i) the policies approved by management which are relevant for SAM have been effectively disseminated throughout the organizational scope defined for the purposes of this part of ISO/IEC 19770				
ii) the processes and procedures which are relevant for SAM, as approved by management, have been effectively implemented throughout the organizational scope defined for the purposes of this part of ISO/IEC 19770				
5) to summarize any exceptions identified and actions which may need to be taken as a result of the above				
6) to identify opportunities for improvement in the provision of services for software and related assets				
7) to consider whether there is a need for a review of policies, processes and procedures as to their continued appropriateness, completeness and correctness.				
b) The SAM owner formally approves the report, documents decisions and actions that are to be taken as a result, and copies it to the corporate board or equivalent body.				●
c) There is a periodic review (at least annually) of whether software and related assets are deployed in the most cost-effective manner possible; and recommendations are made for possible improvement. NOTE 1 This process may be referred to as license optimization. It is to ensure that licensing is maximally cost effective. A value baseline of assets may be used as a base record from which to optimize. A value baseline is the organization's chosen basis to record value of the software, e.g. cost-basis, by which to measure a change over time, allowing the organization to consistently monitor optimization of e.g. value of licenses. NOTE 2 The main coverage for this outcome is in Tier 4. There is limited coverage in Tier 2 to identify immediate opportunities for improvement.		●		●

4.3.5 Continual improvement of SAM

4.3.5.1 Objective

The objective of the *Continual improvement of SAM* process is to ensure that opportunities for improvement are identified and acted upon where considered justified, both in the use of software and related assets and in the SAM processes themselves.	Applicable to Tier 4

4.3.5.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Continual improvement of SAM* process will enable the organization to demonstrate that:				
a) A mechanism is in place to collect and record suggested improvements in SAM arising from all sources throughout the year.				●
b) Suggestions for improvement are periodically assessed, prioritized and approved for incorporation in SAM implementation and improvement plans.				●

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

4.4 Inventory processes for SAM

4.4.1 General

Inventory processes for SAM create and maintain all stores and records for software and related assets, and provide the data management functionality which ensures the integrity of control of software and related assets in the other SAM processes.

Inventory processes for SAM are the basis not only for SAM, but for all of configuration management. Configuration management goes beyond the scope of SAM insofar as it covers all IT assets (not only software and related assets), may cover non-IT assets, and the relationships between all of these assets. In the context of a program encompassing all of IT service management, *Inventory processes for SAM* would be considered part of configuration management.

They need to be performed on a regular basis for the proper functioning of the entire SAM process, and for any IT service management processes that rely on them.

NOTE Standardized information structures such as those specified by other parts of this International Standard will facilitate information processes for SAM, including their automation.

The *Inventory processes for SAM* consist of the following process areas:

a) *Software asset identification*;

b) *Software asset inventory management*;

c) *Software asset control*

4.4.2 Software asset identification

4.4.2.1 Objective

The objective of the *Software asset identification* process is to ensure that the necessary classes of assets are selected and grouped; and defined by appropriate characteristics that enable effective and efficient control of software and related assets.	Applicable to tiers 1 and 4

4.4.2.2 Outcomes

Outcome	Tier			
	1	2	3	4
Implementation of the *Software asset identification* process will enable the organization to demonstrate that:				
a) Types of assets to be controlled and the information associated with them are formally defined, taking into account the following:				•
1) Items to be managed are chosen using established selection criteria, grouped, classified and identified to ensure that they are manageable and traceable throughout their lifecycle. NOTE Business and safety critical assets and high risk assets need to be prioritized and may be controlled at a more detailed level.				
2) Items to be managed include:				
i) All devices or platform instances on which software can be installed or run				
ii) Software definitive master versions and distribution copies				

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
iii) Software builds and releases (originals and distribution copies)				
iv) All installed software				
v) Software versions				
vi) Methodology by which software within scope is identified NOTE Suitable information may be extracted from suitably defined and maintained Software Identification Tags as specified by other parts of this International Standard.				
vii) Patches and updates				
viii) Licenses including underlying licenses and effective full licenses				
ix) Proof of license documentation				
x) Contracts (including metrics, terms and conditions) relating to software assets, including both hard-copy and electronic				
xi) Both physical and electronic stores of the above, as relevant				
xii) Licensing models				
3) Software shall be manageable both by files and by packages corresponding to specific products released by software manufacturers or developers.				
4) Basic information required for all assets is				
i) Unique identifier				
ii) Name/description				
iii) Location				
iv) Custodianship (or owner)				
v) Status (e.g. test/production status; development or build status)				
vi) Type (e.g. software, hardware, facility)				
vii) Version (where applicable)				
NOTE 1 Data validation requirements may also be defined as part of this process. NOTE 2 This information may be extracted from a suitably defined and maintained Software Identification Tag. (See 19770-2).				
b) A register of stores and inventories exists, clarifying which stores and types of information are held, with duplication allowed only if duplicate information can be traced back to the definitive source record. NOTE Typically this register will include the following types of information about each physical collection of stored assets or list of assets i.e. each store or inventory: 1) the defined type of SAM asset: 2) the name of the person who is in charge of managing this information; and 3) the location where this store or inventory can be consulted.	•			

4.4.3 Software asset inventory management

4.4.3.1 Objective

The objective of the *Software asset inventory management* process is to ensure that physical instances of software assets are properly stored; and that required data about characteristics for all assets and configuration items is accurately recorded throughout the life cycle. It also provides information on software assets and related assets to support the effectiveness and efficiency of other business processes.	Applicable to tiers 1 and 4

Documents
Document Sharing Hub

© ISO/IEC 2012 – All rights reserved

Full document details: BS ISO/IEC 19770-1:2012

4.4.3.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Software asset inventory management* process will enable the organization to demonstrate that:				
a) Policies and procedures are developed, approved and issued which include the management and maintenance of inventories and physical/electronic stores including access controls which:	●			
1) protect them from unauthorized access, change or corruption.				
2) provide a means for disaster recovery.				
b) Inventories exist of:	●			
1) all devices or platform instances on which software assets can be installed or run.				
2) all authorized installed software showing (a) packages and versions which can be individually licensed or authorized for deployment; and (b) update/patch status of software; all by platform on which installed. NOTE The inventory of software authorized for installation (or use) is an important reference which unambiguously determines what software is authorized to be installed and to determine whether any given instance of a platform/device may have software used or installed on it. The authorization may be at any level, e.g. at the level of the device, class of user, or organization-wide.				
3) underlying licenses and effective full licenses held. NOTE There is no requirement for separate inventories of underlying and effective full licenses, but there is a requirement to be able to differentiate between the two.				
c) Inventories and corresponding physical/electronic stores exist of:				
1) software (definitive master versions and distribution copies)	●			
2) software builds and releases (originals and distribution copies)				●
3) contracts relating to software assets, both hard-copy and electronic	●			
4) proof of license documentation.	●			
d) Inventories or other clearly defined analysis or metric mechanisms exist to determine any licensing usage based on criteria other than software installations. NOTE These requirements will depend on the licensing models of software being used. For example, they might include metrics such as personnel counts for specified parts of the organization; counts of PCs meeting specified criteria; numbers of users or terminals accessing server resources; numbers of processors; and power of processors.	●			
e) Arrangements are made to ensure the continued availability of the inventory sources and stores listed above.				●
f) Each inventory report produced has a clear description including its identity, purpose, and details of the data source.				●

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 19770-1:2012

4.4.4 Software asset control

4.4.4.1 Objective

The objective of the *Software asset control* process is to provide the control mechanism over software assets and changes to software and related assets while maintaining a record of changes to status and approvals.	Applicable to Tier 4

4.4.4.2 Outcomes

Outcome	Tier			
	1	2	3	4
Implementation of the *Software asset control* process will enable the organization to demonstrate that:				
a) An audit trail is maintained of changes made to software and related assets including changes in the status, location, custodianship and version				•
b) Policies and procedures are developed, approved and issued for the development, maintenance and management of software versions, images/builds and releases.				•
c) Policies and procedures are developed, approved and issued which require that a baseline of the appropriate assets is taken before a release of software to the live environment in a manner that can be used for subsequent checking against actual deployment.				•

4.5 Verification and compliance processes for SAM

4.5.1 General

Verification and compliance processes for SAM detect and manage all exceptions to SAM policies, processes, and procedures; including license use rights.

Verification and compliance processes for SAM are important functions for an organization. They refer to self-audit and self-assessment processes conduct by the organization itself and not to audits conducted by external parties although there are similarities. They need to be performed on a regular basis for the proper functioning of the entire SAM process, and for any IT service management processes that rely on them.

The *Verification and compliance processes for SAM* consist of the following process areas:

a) *Software asset record verification*;

b) *Software licensing compliance*;

c) *Software asset security compliance*;

d) *Conformance verification for SAM*.

4.5.2 Software asset record verification

4.5.2.1 Objective

The objective of the *Software asset record verification* process is to ensure that records reflect accurately and completely what they are supposed to record, and conversely that what they record has not changed without approval.	Applicable to tiers 1, 2 and 4

AVA Documents
Document Sharing Hub

© ISO/IEC 2012 – All rights reserved

Full document details: BS ISO/IEC 19770-1:2012