INTERNATIONAL STANDARD

ISO/IEC 19770-1

Second edition
2012-06-15

Information technology — Software asset management —

Part 1: Processes and tiered assessment of conformance

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

Partie 1: Procédés et évaluation progressive de la conformité

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

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

This second edition cancels and replaces the first edition (ISO/IEC 19770-1:2006), which has been technically revised.

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

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

— *Part 2: Software identification tag*

The following parts are under preparation:

— *Part 3: Software entitlement tag*

— *Part 5: Overview and vocabulary*

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

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

Introduction

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

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

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

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

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

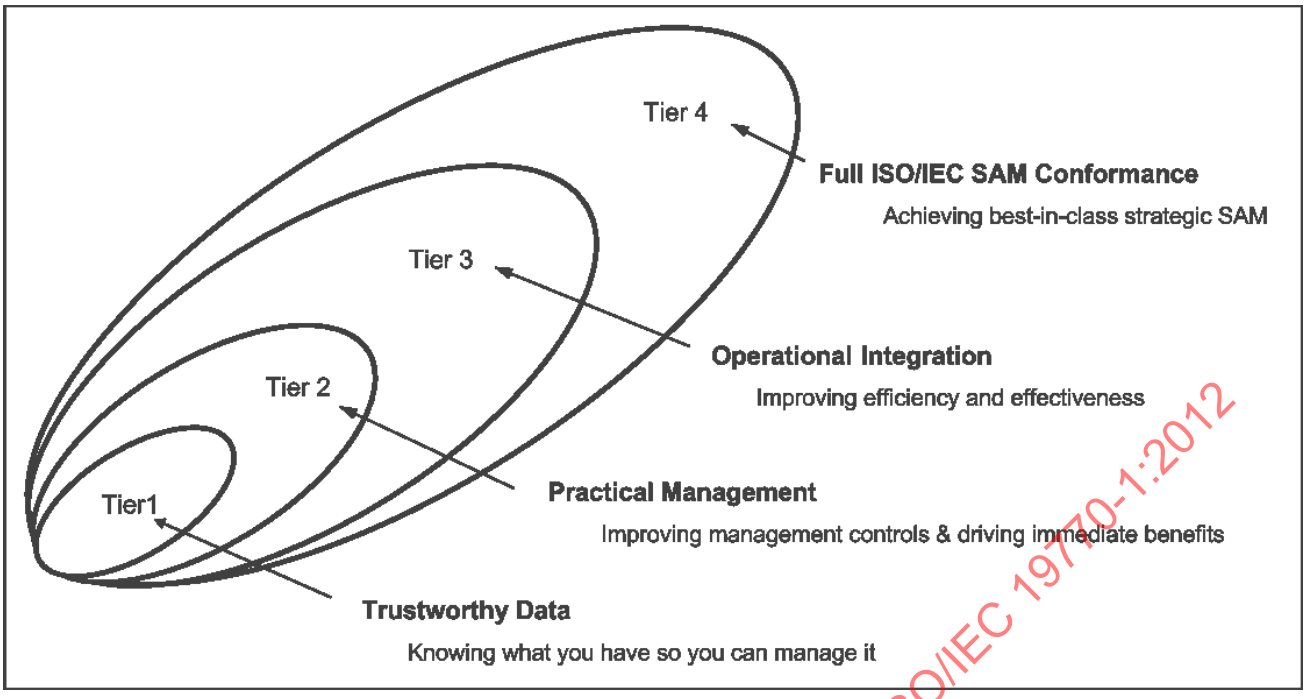

Figure 1 — The four tiers of SAM

The major associated benefits of each tier are:

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

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

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

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

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

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

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

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

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

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

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

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

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

The overall benefits of SAM should include:

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

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

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

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

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

Information technology — Software asset management —

Part 1:
Processes and tiered assessment of conformance

1 Scope

1.1 Purpose

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

1.2 Field of application

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

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

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

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

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

This part of ISO/IEC 19770 can be applied to all software and related assets, regardless of the nature of the software, where related assets are all other assets with characteristics which are necessary to use or manage software. For example, it can be applied to executable software (such as application programs, operating systems and utility programs) and to non-executable software (such as fonts, graphics, audio and video recordings, templates, dictionaries, documents and data). It can be applied to all technological environments and computing platforms (e.g., virtualized software applications, on-premises or software-as-a-service; it is equally relevant in cloud computing as it is in older computing environments).

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

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

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

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

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

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

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

c) media holding copies of software for use.

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

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

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

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

1.3 Limitations

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

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

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

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

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

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.

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

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

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.

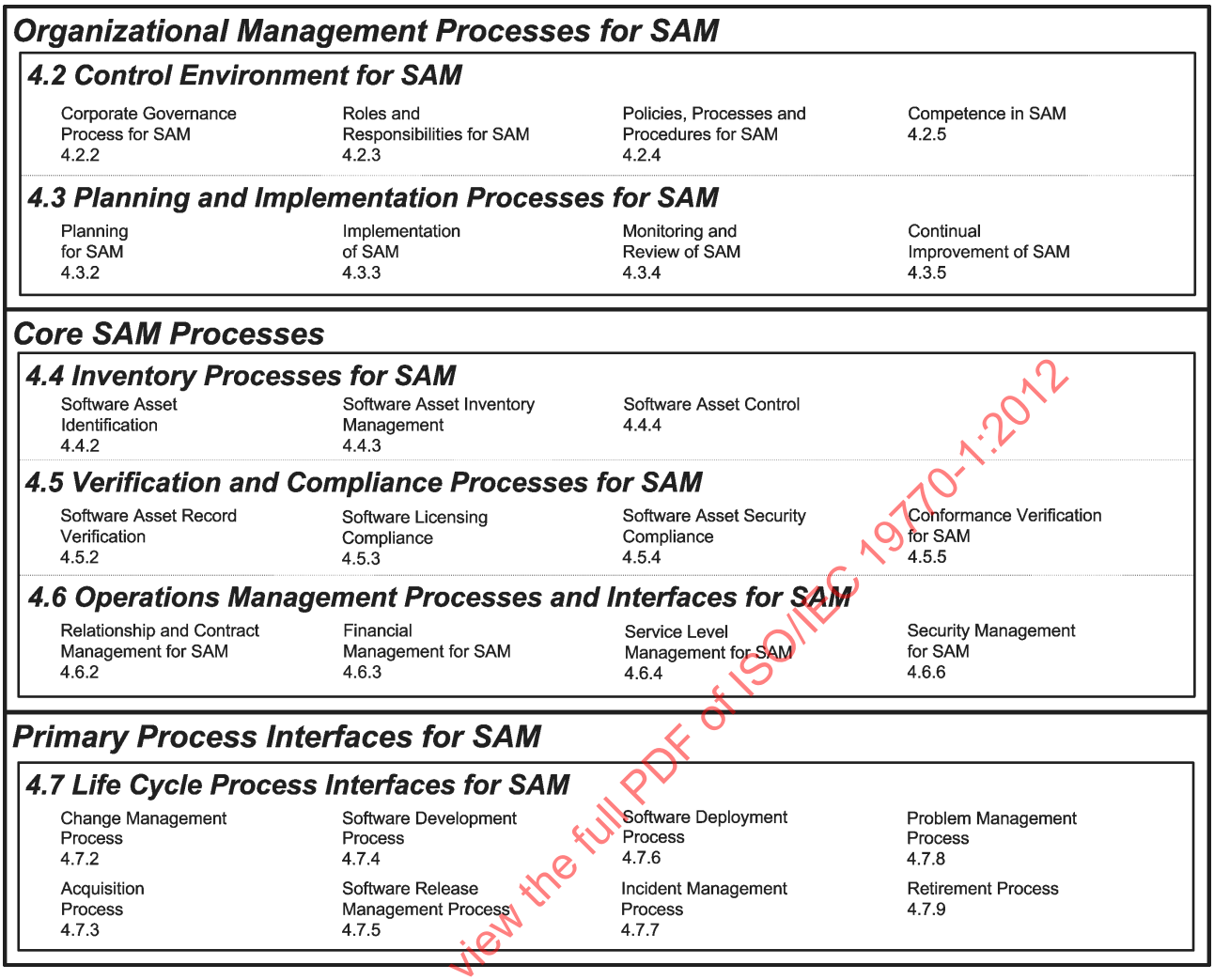

Figure 2 — Framework for SAM processes

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.

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

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.				•

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	Tier 2	Tier 3	Tier 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.		•		

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.		•		

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	2	3	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*.

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	Tier 2	Tier 3	Tier 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.		•		

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	Tier 2	Tier 3	Tier 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	Tier 2	Tier 3	Tier 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				

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.				•

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	Tier 2	Tier 3	Tier 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				

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

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.				•

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

4.5.2.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Software asset record verification* process will enable the organization to demonstrate that:				
a) Procedures are developed, approved and issued for the *Software asset record verification* process to include:				
1) Whenever scope is defined or changed, there is a validation of that scope by reviewing contract and purchase history in order to ensure the organizational and software scopes are aligned with business requirements. NOTE For example, such a review is required when another software manufacturer is included in scope, or when there is a merger or demerger of the organization using the standard, or a change of ownership of software among software manufacturers.	•			
2) At least quarterly there is reconciliation between what is installed on each device or platform instance and what was authorized for installation, including reporting on exceptions identified in what is currently installed, and in what has changed since the previous reconciliation. NOTE Some changes may be explained by updates in the methodology by which software is identified (e.g. updated signature files, so that a product previously reported as a single application is now properly identified as part of a suite.)	•			
3) The hardware inventory including locations is verified at least 6-monthly, including reporting on exceptions identified.	•			
4) The inventory of software programs (definitive master versions and distribution copies) is verified at least 6-monthly, including reporting on exceptions identified.				•
5) The inventory of software builds (originals and distribution copies) is verified at least 6-monthly, including reporting on exceptions identified.				•
6) The physical store of proof of license documentation is verified (including for authenticity) at least annually, including reporting on exceptions identified.				•
7) The bases for and calculations of effective licenses from underlying licenses are reviewed at least annually, to ensure that necessary underlying licenses exist and that quantities are not being double-counted.				•
8) The physical store of contractual documentation related to software assets is verified for completeness at least annually, including reporting on exceptions identified.	•			
9) The contracts inventory is verified at least annually, including reporting on exceptions identified.	•			
10) There is a periodic review of historical invoices for the purpose of identifying incorrect billing and overpayment. NOTE This may be considered part of conformance verification but is more extensive and more formal than what is required for conformance verification.		•		
11) Follow-up corrective actions on any discrepancies or issues identified above take place and are documented. Note: as new verifications are encountered in successive tiers, so new follow-ups must be demonstrated in this tier, as indicated.	•	•		•

4.5.3 Software licensing compliance

4.5.3.1 Objective

The objective of the *Software licensing compliance* process is to ensure that all intellectual property used by the organization but owned by others, pertaining to software and related assets, is properly licensed and used in accordance with its terms and conditions.	Applicable to Tier 1

4.5.3.2 Outcomes

Outcome	Tier 1	2	3	4
Implementation of the *Software licensing compliance* process will enable the organization to demonstrate that:				
a) Procedures are developed, approved and issued for the *Software licensing compliance* process to include the following:	•			
1) Reconciliation is conducted at least quarterly between effective licenses owned and licenses required for software used, taking into account the way licensing requirements are determined as per license terms and conditions. NOTE 1 This includes in particular license requirements determined on bases other than installed copies, such as server access rights. NOTE 2 The quarterly cycle of reconciliation is primarily a process of analysis and calculation, using measurement of licenses required and quantities from inventories and documented actual installs to calculate where more or less licenses are required. It is expected that terms and conditions are reviewed at least annually, with further checks within three months where new measures or license models are found to apply, where scope has changed, or where a manufacturer announces specific changes to license terms.				
2) Discrepancies identified in this reconciliation are promptly recorded, analyzed and the root cause is determined.				
3) Follow up actions are prioritized and executed.				

4.5.4 Software asset security compliance

4.5.4.1 Objective

The objective of the *Software asset security compliance* process is to ensure that security requirements related to the use of software and related assets are complied with.	Applicable to Tier 3

4.5.4.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Software asset security compliance* process will enable the organization to demonstrate that:				
a) Actual practice is reviewed at least annually to detect security policy exceptions. This verification shall include the verifying of access controls on software definitive master versions and distribution copies of software; and installation/usage rights specified by user or user group.			•	
b) Follow-up on any discrepancies identified in this review takes place and is documented.			•	

4.5.5 Conformance verification for SAM

4.5.5.1 Objective

The objective of the *Conformance verification for SAM* process is to ensure that there is continuing compliance with the requirements of this part of ISO/IEC 19770 including compliance with required policies and procedures. NOTE This is one of the most important process areas specified in this part of ISO/IEC 19770, as it provides assurance that the other processes are functioning as expected. It is effectively self-verification, with a requirement to retain evidence of the checks performed. Although each tier is defined 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. Conformance to 4.5.5.2 (conformance verification) is assessed by checking the self-verification of all other outcomes at the desired tier."	In all tiers for the requirements of that tier.

4.5.5.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Conformance verification for SAM* process will enable the organization to demonstrate that:				
a) Policies and procedures are developed, approved and issued for verifying compliance with the relevant tier(s) of this part of ISO/IEC 19770, which ensure verification at least on a sample basis annually against all of the requirements specified in the relevant tier(s) of this part of ISO/IEC 19770. This shall include verification that procedures implemented by the organization for other SAM processes are meeting all requirements specified in this part of ISO/IEC 19770 for those procedures.	•	•	•	•
b) Documentary evidence exists that demonstrates (a) that the verification procedures above are being performed, and (b) that corrective follow-up action is taken until successful completion on the causes of all identified exceptions.	•	•	•	•

4.6 Operations management processes and interfaces for SAM

4.6.1 General

Operations management processes and interfaces for SAM execute operational management functions which are essential to achieving overall SAM objectives and benefits.

The *Operations management processes and interfaces for SAM* consist of the following process areas:

a) *Relationship and contract management for SAM*;

b) *Financial management for SAM*;

c) *Service level management for SAM*;

d) *Security management for SAM*.

4.6.2 Relationship and contract management for SAM

4.6.2.1 Objective

The objective of the *Relationship and contract management for SAM* process is to manage relationships with other organizations, both external and internal, to ensure the provision of seamless, quality SAM services, and to manage all contracts for software and related assets and services. NOTE *Relationship and contract management for SAM* will typically operate closely together with *Service level management for SAM* since service levels will typically be defined to help manage such relationships	Applicable to tiers 2, 3 and 4

4.6.2.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Relationship and contract management for SAM* process will enable the organization to demonstrate that:				
a) Policies and procedures are developed, approved and issued for managing relationships with suppliers providing software and related assets and services, to include:			•	
1) Definitions of responsibilities for supplier management with individuals assigned to have clear overall responsibility for managing each supplier.				
2) Developing invitations to tender for the supply of software or related services; to ensure that the process includes consideration of requirements for SAM, including service level management, security controls, release and change management.				
3) Formal documented reviews at least 6-monthly of supplier performance, achievements and issues, with documented conclusions and decisions about any actions to be taken.				
b) Policies and procedures are developed, approved and issued for managing customer-side relationships, to include:				•
1) Definitions of responsibilities for managing customer-side business relationships with respect to software and related assets and services.				

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
2) A formal review at least annually of current and future software requirements of customers and the business as a whole.				
3) Formal documented reviews at least annually of service provider performance, customer satisfaction, achievements and issues, with documented conclusions and decisions about any actions to be taken.				
c) Policies and procedures are developed, approved and issued for managing contracts, to include:				
1) Ensuring that contractual details are recorded in an on-going contract management system as contracts are signed. NOTE The contract management system can be an in-house developed manual or electronic system that permits management and control of contracts.			•	
2) Holding copies of all signed contractual documentation securely with copies kept in a document management system. NOTE Optionally this may include the terms and conditions accepted electronically when third-party software is installed.			•	
3) Documented reviews at least 6-monthly and also prior to contract expiry, of all contracts for software and related assets and services, with documented conclusions and decisions about any actions to be taken. NOTE The main coverage for this outcome is in Tier 3. There is limited coverage in Tier 2 to identify immediate opportunities for improvement, including in particular for maintenance on software not being used, and opportunities for improved purchasing arrangements.		•	•	

4.6.3 Financial management for SAM

4.6.3.1 Objective

The objective of the *Financial management for SAM* process is budgeting and accounting for software and related assets; and ensuring that relevant financial information is readily available for financial reporting, tax planning, and calculations such as total cost of ownership and return on investment. NOTE *Financial management for SAM* does not cover charging. In practice, many organizations will be involved in charging for software and related assets and related services. However, since charging is an optional activity, it is not covered by this part of ISO/IEC 19770. It is recommended that where charging is in use, the mechanism for doing so is fully defined and understood by all parties.	Applicable to tiers 2 and 3

4.6.3.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Financial management for SAM* process will enable the organization to demonstrate that:				
a) Definitions of financial information relevant to the management of software and related assets are agreed with relevant parties and documented by asset type. NOTE1 Financial classification of costs associated with software and related assets is an important part of Financial Management for SAM. The asset types used in financial management should be aligned with or mapped to the asset types in SAM if there are differences. NOTE2 Data requirements for asset types are formally defined in Tier 4. These will be evolved throughout Tiers 1-3. (See *4.4.2 Software asset identification*).			•	
b) Formal budgets are developed for the acquisition of software assets (externally or internally) and the related support and infrastructure costs.			•	
c) Actual expenditure on software assets and the related support and infrastructure costs is accounted for against budget.			•	
d) Clearly documented financial information is readily available about software asset values (including historical cost and depreciated cost).			•	
e) There are formal documented reviews at least quarterly of actual expenditure against budget, with documented conclusions and decisions about any actions to be taken.			•	
f) License optimization is performed, consisting of cost-benefit analysis of drivers of licensing costs, and resulting in recommendations for improvement. NOTE1 For example, a low-value business application such as a staff directory utility which consumes high-cost licenses for every user might be replaceable by an alternative less expensive approach to achieving the same business objective. NOTE2 The main coverage for this outcome is in Tier 3. There is limited coverage in Tier 2 to identify and document immediate opportunities for improvement. Tier assessments are on this basis.		•	•	

4.6.4 Service level management for SAM

4.6.4.1 Objective

The objective of the *Service level management for SAM* process is to define, record and manage levels of service related to SAM.	Applicable to Tier 3

4.6.4.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Service level management for SAM* process will enable the organization to demonstrate that:				
a) Service level agreements and supporting agreements are developed and approved for services that are performed within the scope of SAM; to include that:			•	
1) Services relating to software acquisition, installation, moves, and changes of software assets and related assets are defined and agreed with relevant parties together with the corresponding service level targets and workload characteristics.				
2) The customer and user obligations and responsibilities in relation to SAM are defined or referenced from the service level agreement. NOTE Service Level Agreements covering requirements for SAM could cover more than just SAM.				
b) Actual workloads and service levels against targets for SAM are reported regularly (at least quarterly), and the reasons for non-conformance are documented.			•	
c) Regular reviews (at least quarterly) by the relevant parties are held to review performance against service levels for SAM with documented conclusions and decisions about any actions to be taken.			•	

4.6.5 Security management for SAM

4.6.5.1 Objective

The objective of the *Security management for SAM* process is to manage information security effectively within all SAM activities and support the approval requirements related to SAM. NOTE ISO/IEC 27001 provides guidance on information security management. Organizations certified to ISO/IEC 27001 will normally satisfy the security requirements within this part of ISO/IEC 19770.	Applicable to Tier 4

4.6.5.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Security management for SAM* process will enable the organization to demonstrate that:				
a) A formal policy is developed and approved regarding security/access restrictions to all SAM resources, including physical/electronic stores of software, software builds and releases. NOTE Advancing to full conformance requires more active management of access rights to all SAM resources including documents and inventories (Tier 3 requirements may be met by periodic verifications of controls. Refer to software asset security compliance outcomes (a) and (b) in 4.5.4.)				•
b) Access controls are specified, both physical and logical, to enforce the approval requirements of SAM policies.				•
c) There is documentary evidence that these specified access controls are being implemented in practice.				•

4.7 Life cycle process interfaces for SAM

4.7.1 General

The *Life cycle process interfaces for SAM* are largely aligned to the primary life cycle processes of ISO/IEC 12207 in the context of SAM as well as to ISO/IEC 20000. This part of ISO/IEC 19770 specifies SAM requirements for these life cycle processes.

The *Life cycle process interfaces for SAM* consist of requirements for the following life cycle process areas:

a) *Change management process*;

b) *Acquisition process*;

c) *Software development process*;

d) *Software release management process*;

e) *Software deployment process*;

f) *Incident management process*;

g) *Problem management process*;

h) *Retirement process*.

4.7.2 Change management process

4.7.2.1 Objective

The objective of the *Change management process* with respect to software and related assets is to ensure that all changes which impact on SAM are assessed, approved, implemented and reviewed in a controlled manner and meet all record-keeping requirements. NOTE The *Change management process* with respect to software and related assets is tightly linked to the *Software asset control* process, which provides the control mechanism underlying any changes to be made to software and related assets.	Applicable to Tier 4

4.7.2.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Change management process* will enable the organization to demonstrate that:				
a) There is a formal process of change management which includes:				•
1) All change requests that affect software or related assets or services, or SAM processes, are identified and recorded.				
2) Change requests affecting software or related assets or services, or SAM processes, are assessed for possible impacts, prioritized, and approved by the responsible management.				
3) The process implementing the approved change request does so only in accordance with the approval.				
4) All changes affecting software or related assets or services, or SAM processes, are recorded.				
5) The success or failure of such changes is documented and periodically reviewed.				

4.7.3 Acquisition process

4.7.3.1 Objective

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 properly recorded.	Applicable to Tier 3

4.7.3.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Acquisition process* will enable the organization to demonstrate that:				
a) Standard architectures are defined for the provision of software services, as are the criteria for deviating from those standards.			•	
b) Standard software configurations are defined, as are the criteria for deviating from those standards.			•	
c) Policies and procedures are developed, properly authorized and issued for requisitioning and ordering software assets and related assets, including:			•	
1) How requirements are specified.				
2) Management and technical approvals required.				
3) Use/redeployment of existing licenses if available. NOTE The organization may choose the best method for itself for identifying if there are existing licenses available for deployment. Depending on how the organization implements software asset management, this may vary. For example, software may be authorized for installation but not yet be installed. To avoid the risk of trying to use the same licenses more than once, authorizations and ongoing deployment activities may need to be checked before redeploying licenses.				
4) Recording future purchase requirements in those cases where software can be deployed before reporting and payment.				
d) Policies and procedures are developed, properly authorized and issued for receipt-processing functions related to software and related assets, including:			•	
1) Processing invoices, including reconciliations to orders and retention of copies for license management purposes.				
2) Ensuring the receipt and safe-keeping of valid proof of license for all licenses purchased. NOTE This may require checking for authenticity of proof of license, i.e. checking that they are not counterfeit, especially when the proof of license is not received directly from the relevant software manufacturer.				
3) Processing incoming media which includes requirements for verification, record-keeping and safe-keeping of contents (physical media and electronic copies).				

4.7.4 Software development process

4.7.4.1 Objective

The objective of the *Software development process* in respect of software and related assets is to ensure that they are developed in a way which considers SAM requirements. NOTE 1 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 source code or other components in development. It is intended that it be applied to all software used to facilitate these development environments, transitions to live environments and precursor activities such as configuring software and creating and controlling production builds and releases. The line between what is considered source software within pure development, and therefore excluded, and software for use, and therefore included, may be defined as part of a formal scope statement. NOTE 2 Software used to develop other software is considered software for use, i.e. the software used by software developers must itself be controlled.	Applicable to Tier 4

4.7.4.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Software development process* will enable the organization to demonstrate that:				
a) There is a formal process for software development ensuring the following have been considered:				•
1) Standard architectures and standard configurations.				
2) License constraints and dependencies.				
b) There is a formal process for software development ensuring that software products are placed under software asset control before being introduced into a live environment.				•

4.7.5 Software release management process

4.7.5.1 Objective

The objective of the *Software release management process* in respect of software and related assets is to ensure that releases are planned and executed in a way which supports SAM requirements. NOTE The *Software release management process* covers the planning and actual release of software and related assets. The *Software release management process* is closely related to the *Change management process* and they should be procedurally connected.	Applicable to Tier 4

4.7.5.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Software release management process* will enable the organization to demonstrate that:				
a) There is a formal process for release management ensuring that:				●
1) A controlled acceptance environment is used to build and test all proposed releases including patches prior to release. NOTE This part of ISO/IEC 19770 does not specify the detailed requirements for build or testing. For example, it does not require that all builds requiring a manufacturer patch be rebuilt and independently tested, although an organization may require this independently of what this part of ISO/IEC 19770 requires. Nonetheless, it would normally be expected that any change or patch would be tested before deployment.				
2) The frequency and type of releases are planned and agreed with the business and customers, including the frequency of security patch releases.				
3) The planned release dates and deliverables are recorded with references to related change requests and problems, and communicated to incident management.				
4) The release of software and related assets is approved by the responsible management.				
5) The success or failure of releases is recorded, and periodically reviewed.				

4.7.6 Software deployment process

4.7.6.1 Objective

The objective of the *Software deployment process* in respect of SAM is to ensure that software deployment and redeployment is executed in a way which supports SAM requirements.	Applicable to Tier 3

4.7.6.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Software deployment process* will enable the organization to demonstrate that:				
a) Policies and procedures are developed, approved and issued for deploying software to include the following:			●	
1) Any new instance of a distribution copy of software and related assets is approved by the responsible management.				
2) For any deployment there is a back out procedure or method of remediation if the deployment is not successful.				
3) Security requirements are complied with, including over access to the software being deployed and after it is installed.				

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
4) All changes to status of the relevant software and related assets are recorded accurately and on a timely basis, including any change of custodianship for the assets, and an audit trail kept of these changes. NOTE There is no requirement for an audit trail of every single change made. It is essential to define each permissible status used to record all deployment steps, and then ensure that there are audit trails of when any status changes. Typical status changes might be connected with authorization for procurement (general authorization; authorization for named groups or individuals); authorization for release (as part of a build); authorization for deployment/removal (general, and for named groups or individuals); and actual deployment/installation/removal.				
5) There is a documented control to verify that what was deployed is the same as what was authorized to be deployed and an exception raised detailing any variances or if an asset cannot be verified to be deployed within authorized limits. NOTE 1 Authorizations typically change over time. Review of deployment versus authorizations is recommended whenever authorization changes, whether explicit or implicit, such as when there is a change of organizational scope. NOTE 2 It is recommended a copy of the exception report be sent to the owner for the Inventory of Software Authorized for Installation				
6) The success or failure of deployments is recorded, and periodically reviewed.				

4.7.7 Incident management process

4.7.7.1 Objective

The objective of the *Incident management process* in respect of software and related assets is to monitor and respond to incidents in ongoing operations relevant to software and related assets.	Applicable to Tier 4

4.7.7.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Incident management process* will enable the organization to demonstrate that:				
a) There is a formal process of incident management which includes:				•
1) All incidents that affect software or related assets or SAM processes are recorded and classified as to their priority for resolution.				
2) All such Incidents are resolved in accordance with their priority for resolution, and the resolution is documented.				

4.7.8 Problem management process

4.7.8.1 Objective

The objective of the *Problem management process* in respect of software and related assets is to keep software assets current and in operational fitness, including through proactive identification and analysis of the cause of incidents and addressing the underlying problems.	Applicable to Tier 4

4.7.8.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Problem management process* will enable the organization to demonstrate that:				
a) There is a formal process of problem management which includes:				•
1) All incidents that affect software or related assets or services or SAM processes are recorded and classified as to their impact.				
2) High priority and repeat incidents are analyzed for the underlying causes and prioritized for resolution.				
3) Underlying causes are documented and communicated to incident management.				
4) Problems are resolved in accordance with their priority for resolution, and the resolution is documented and communicated to incident management.				

4.7.9 Retirement process

4.7.9.1 Objective

The objective of the *Retirement process* in respect of software and related assets is to remove software and related assets from use, including recycling of associated assets where appropriate, in accordance with company policy and meeting all record-keeping requirements. NOTE Removing unlicensed software from use will generally not resolve a licensing shortfall problem because a licensing obligation has already been created through the use of the software. Reliance should be placed instead on controls over installation or over initial usage.	Applicable to Tier 3

4.7.9.2 Outcomes

Outcome	Tier 1	Tier 2	Tier 3	Tier 4
Implementation of the *Retirement process* will enable the organization to demonstrate that:				
a) Policies and procedures are developed, approved and issued for securely retiring software or hardware on which software is installed, which ensure:			•	
1) Deployed copies of software are removed from retired hardware, except when explicitly authorized by management after due consideration of any software licensing and data confidentiality implications. NOTE 1 For the purposes of this requirement, retirement consists of hardware being transferred outside of the organization potentially to be used by others. NOTE 2 For the purposes of this requirement, deployed software does not include software which is bound to the hardware, such as OEM software which cannot be redeployed.				
2) Licenses and other assets which can be redeployed are identified for redeployment.				
3) Any assets transferred to other parties (whether those parties or related or unrelated, and however transferred, i.e. sold or otherwise) are transferred properly taking into account any confidentiality, licensing, or other contractual requirements.				
4) Licenses and other assets which cannot be redeployed are properly disposed of.				
5) Records are updated to reflect the changes above, and audit trails are maintained of the changes.				

5 Tiers

5.1 Overview

An overview of the tiers is given in the Introduction. *Figure 1* which is included there shows the conceptual relationship between the tiers.

The principles which underlie the groupings and sequencing of the tiers are as follows:

a) **Number of tiers.** There needs to be only a limited number of tiers for conceptual simplicity.

b) **Priority for license compliance.** Formal research into market demand for SAM standards clarified that license compliance was consistently the top priority for all categories of respondents. The first tier, 'Trustworthy Data', provides the basis for repeatable license compliance. It does not guarantee license compliance, but any organization fully conforming to the requirements of Tier 1 will know whether it is compliant with its software licensing, and it will only be a question as to how management is acting on this knowledge.

c) **Natural groupings reflecting natural sequence.** The groupings of outcomes and process areas in each tier are intended to be relatively natural groupings which reflect a natural progression as observed in reality. The actual groupings are described under each tier below in subclauses *5.2* through *5.5*. The supporting principles are as follows:

   1) Having good data almost always comes first. Often this is driven by a vendor-initiated licensing audit. There is often a major gap between what is found and what was believed to be the case. Only then does management typically realize both the significance of exposures and of opportunities for improvement, including in security and in cost savings.

   2) When management does take ownership of SAM issues as a result of having good data, there tend to be two different thrusts to actions taken. Firstly, basic improvements in management controls are instituted, such as clarification of roles and responsibilities, and better definition of policies. Secondly, specific projects are typically initiated to correct problems identified, and to obtain 'quick wins' where possible.

   3) Improvements in efficiency and effectiveness are often cited as expected benefits from SAM, but often are not achieved to the level possible, because they typically require significant implementation effort involving process integration and re-design. However, an organization is more likely to proceed down this path after already seeing the clear benefits of 'quick wins' and recognizing that more are possible.

   4) Best-in-class SAM practices typically come last. These tend to be those practices which have strategic impact and longer-term benefits.

d) **Minimum requirements for recognition.** The tiers are designed to be minimum requirements for recognizable achievement, but do not include everything which an organization may wish to do. For example, policies are not included in Tier 1, but rather only in Tier 2, yet most organizations will probably have some policies in place already during work on Tier 1. This does not diminish the importance of policies, but merely reflects that policies are initially focused upon in Tier 2. Indeed, the findings from achieving Tier 1 will probably drive significant policy development in Tier 2, or at least enforcement, because reality typically will not match expectations in terms of license compliance, security, standardization, etc. Likewise, an organization will probably wish to focus on some specific issues or process areas earlier than required by the tiers, where there are specific requirements or opportunities identified by management. This is to be expected. However, these issues or process areas will not be included in the scope of a potential certification project until the appropriate tier.

e) **Limitations in technology and its use.** There are, for example, hundreds of tools which support software discovery, but far fewer which support full configuration management, and their effective use is still rarer.

The concept of 'difficulty' also needs to be considered:

a) Difficulty per se is not an underlying principle for the grouping and sequencing of tiers. For example, creating and maintaining inventories of software contracts and licenses is not easy, and is typically a highly manual task. Nonetheless it is in Tier 1, because it is one of the critical types of data which must be under control to have trustworthy data.

b) There are many outcomes or process areas which are not typically achieved by less mature organizations, and these have generally been placed in Tier 4. From one perspective, these may be viewed as 'difficult' outcomes and process areas. However, they reflect more about the stage of development of the organization than on their own intrinsic difficulty. Indeed, such outcomes and process areas are more accurately considered part of 'best-in-class' SAM.

5.2 Tier 1 – trustworthy data

Figure 3 shows the process areas which are included in Tier 1.

The natural groupings included in this tier are:

a) Core SAM records

b) License compliance

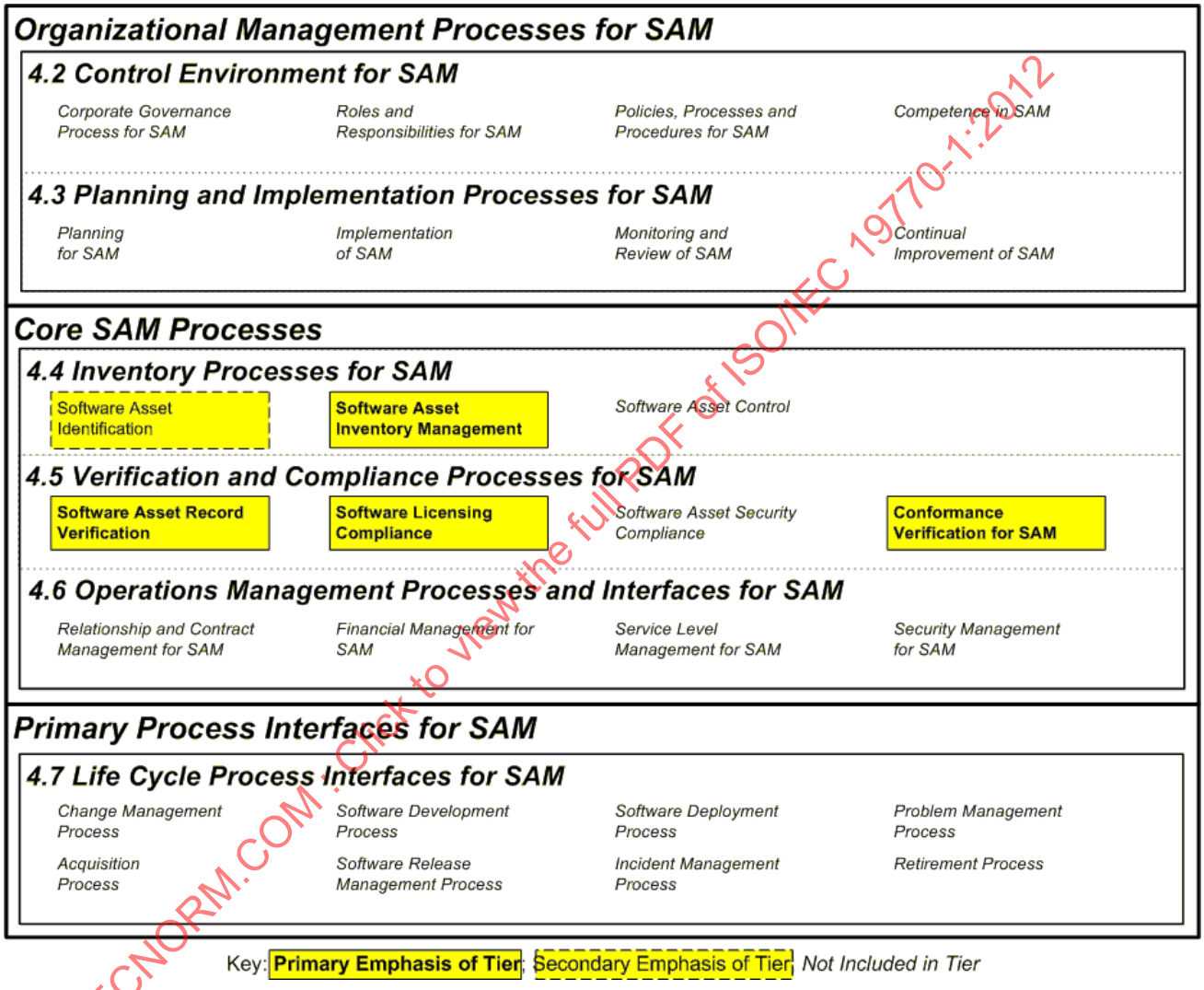

Figure 3 — SAM Tier 1 – trustworthy data

5.3 Tier 2 – practical management

Figure 4 shows the process areas which are included in Tier 2.

The natural groupings included in this tier are:

a) Quick wins

b) Essential control environment

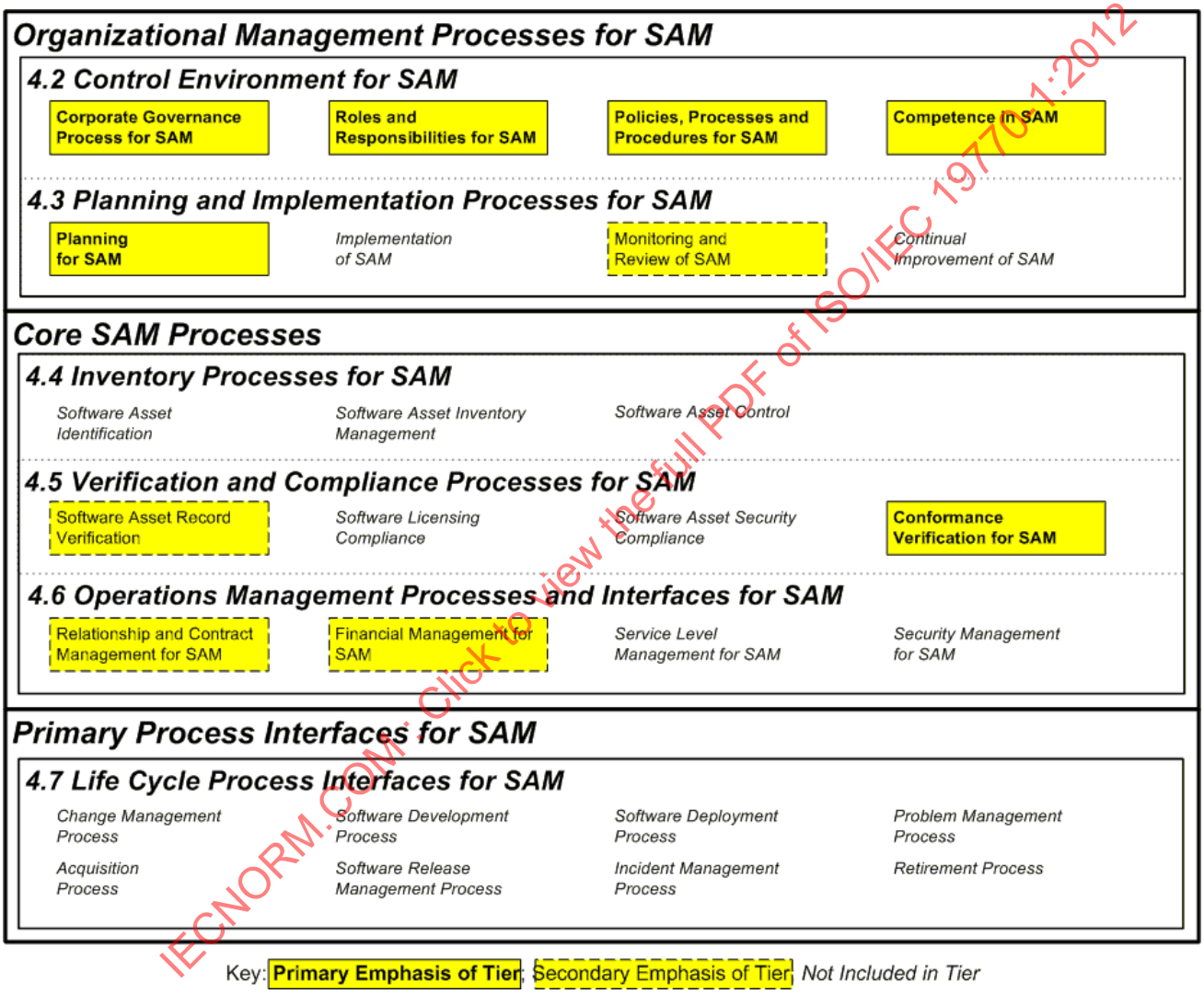

Figure 4 — SAM Tier 2 – practical management

5.4 Tier 3 – operational integration

Figure 5 shows the process areas which are included in Tier 3.

The natural groupings included in this tier are:

a) Core life cycle processes (acquisition/deployment/retirement)

b) Core operations management processes

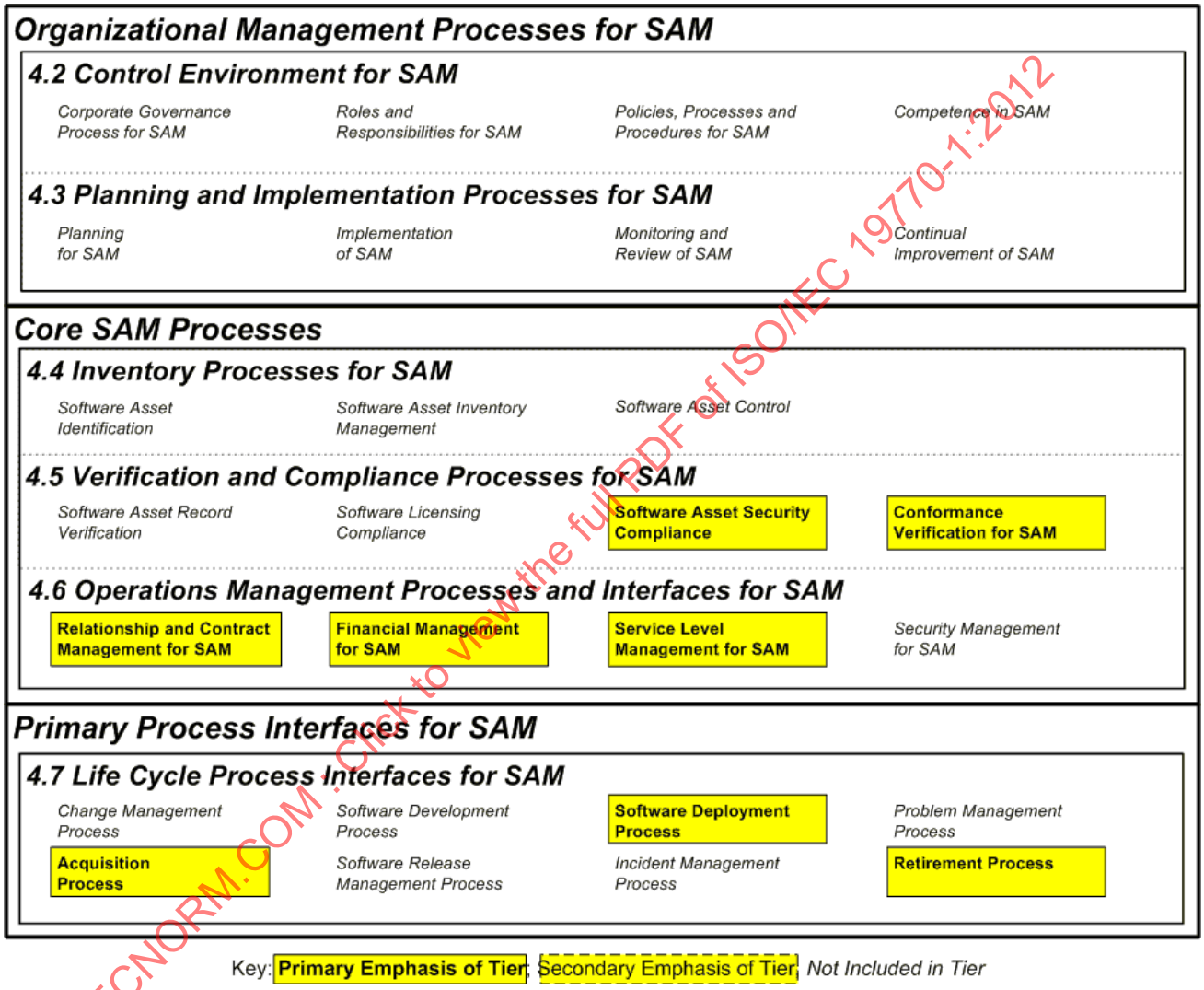

Figure 5 — SAM Tier 3 – operational integration

5.5 Tier 4 – full ISO/IEC SAM conformance

Figure 6 shows the process areas which are included in Tier 4.

The natural groupings included in this tier are:

a) Strategic SAM (SAM is an enabler and part of strategy and planning)

b) Extended Service Management life cycle processes

c) Best-in-class SAM processes (not included in lower tiers)

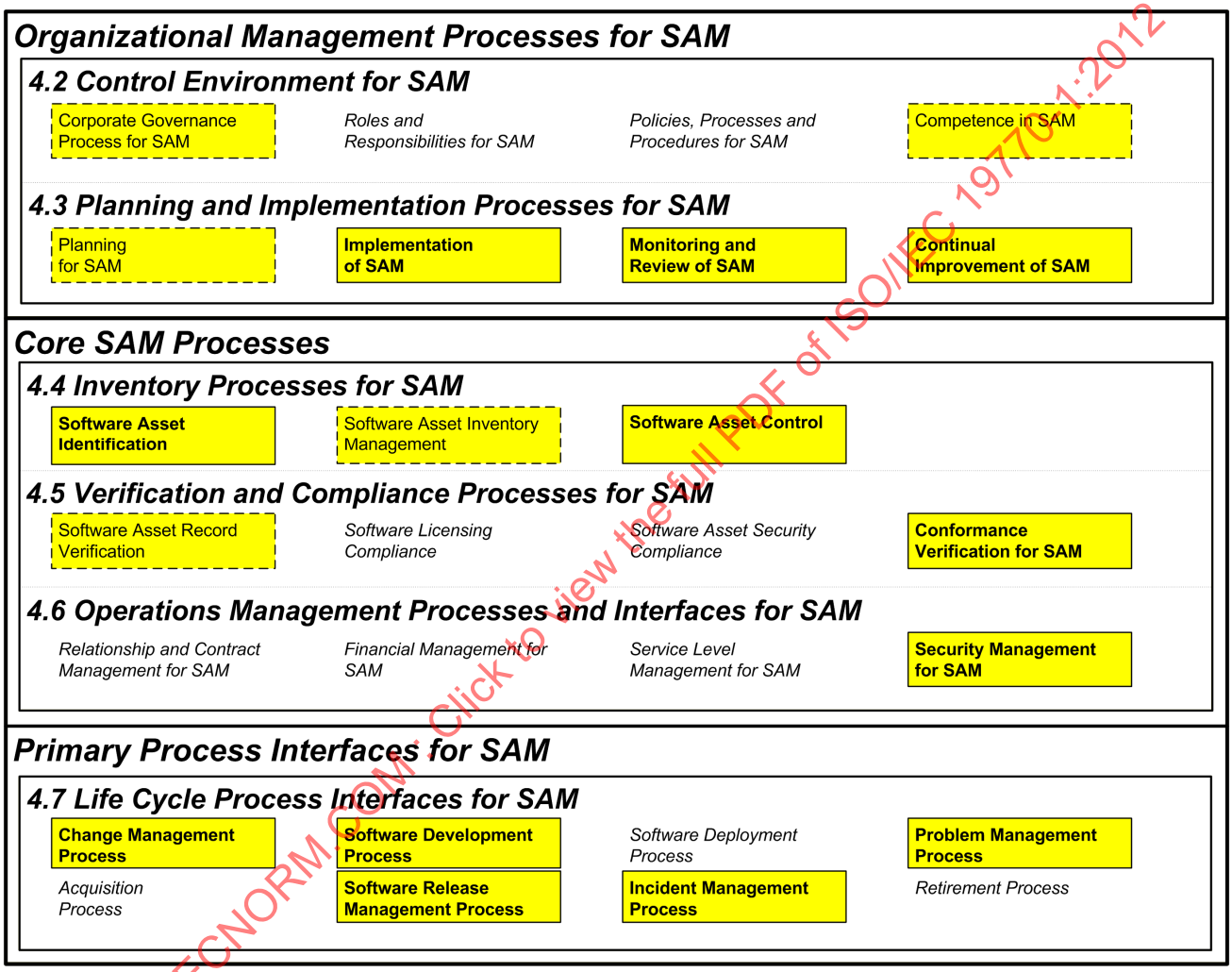

Figure 6 — SAM Tier 4 – full ISO/IEC SAM conformance

Annex A
(informative)

Reference chart of outcomes by tier

Major Name	Minor Name	Process Area Name	Outcome	Caption	Additional Comments	Tier 1	Tier 2	Tier 3	Tier 4
Organizational Management Processes for SAM	Control Environment for SAM	Corporate Governance Process for SAM	4.2.2.2.a	Organizational scope and overall responsibility			x		
			4.2.2.2.b	Recognition of responsibility for SAM			x		
			4.2.2.2.c	Legislation, regulation and guidance			x		
			4.2.2.2.d	Risk assessment			x		
			4.2.2.2.e	Approval of SAM management objectives					x
		Roles and Responsibilities for SAM	4.2.3.2.a	Organization-wide SAM responsibilities			x		
			4.2.3.2.b	Local SAM responsibilities			x		
			4.2.3.2.c	Communication of responsibilities			x		
		Policies, Processes and Procedures for SAM	4.2.4.2.a	Structured approach to policies, processes and procedures			x		
			4.2.4.2.b	Organization of policies, processes and procedures			x		
			4.2.4.2.c	Issues covered by policies			x		
			4.2.4.2.d	Communication of policies and procedures			x		
		Competence in SAM	4.2.5.2.a	Availability of training			x		
			4.2.5.2.b	Proof of license					x
			4.2.5.2.c	Training taken			x		
			4.2.5.2.d	Availability of guidance from software manufacturers			x		
	Planning and Implementation Processes for SAM	Planning for SAM	4.3.2.2.a	Development of SAM management objectives					x
			4.3.2.2.b	Development of SAM plans			x		
			4.3.2.2.c	Approval of SAM plans			x		
		Implementation of SAM	4.3.3.2.a	Issue feedback					x
			4.3.3.2.b	Progress against SAM plan					x
			4.3.3.2.c	Follow-up on variances					x
		Monitoring and Review of SAM	4.3.4.2.a	Annual management review of SAM					x
			4.3.4.2.b	SAM owner sign-off					x
			4.3.4.2.c	Software deployment review			partial (quick wins)		full
		Continual Improvement of SAM	4.3.5.2.a	Suggestions for improvement feedback					x
			4.3.5.2.b	Suggestions for improvement execution					x

Major Name	Minor Name	Process Area Name	Outcome	Caption	Additional Comments	Tier 1	Tier 2	Tier 3	Tier 4
Core SAM Processes	Inventory Processes for SAM	Software Asset Identification	4.4.2.2.a	Initial identification of data requirements					x
			4.4.2.2.b	Master register of stores and inventories		x			
		Software Asset Inventory Management	4.4.3.2.a	Policies and procedures for inventory management		x			
			4.4.3.2.b	Inventories of hardware, installed software, and licenses		x			
			4.4.3.2.c	Inventories of software masters and contractual documentation		1, 3-4			2
			4.4.3.2.d	Measurement mechanisms for all other licensing metrics		x			
			4.4.3.2.e	Continuity of operations					x
			4.4.3.2.f	Minimum report descriptors					x
		Software Asset Control	4.4.4.2.a	Audit trail of changes					x
			4.4.4.2.b	Policies and procedures for version control					x
			4.4.4.2.c	Policies and procedures for deployment baselines					x
	Verification and Compliance Processes for SAM	Software Asset Record Verification	4.5.2.2.a	Policies and procedures for record verification	11 in all Tiers for relevant processes	1-3, 8-9	10 (quick wins)		4-7
		Software Licensing Compliance	4.5.3.2.a	Policies and procedures for software licensing compliance		x			
		Software Asset Security Compliance	4.5.4.2.a	Execution of SAM security policy checks				x	
			4.5.4.2.b	Follow-up on exceptions identified				x	
		Conformance Verification for SAM	4.5.5.2.a	Policies and procedures for conformance verification	In all Tiers for relevant processes	x	x	x	x
			4.5.5.2.b	Execution of conformance verification	In all Tiers for relevant processes	x	x	x	x
	Operations Management Processes and Interfaces for SAM	Relationship and Contract Management for SAM	4.6.2.2.a	Policies and procedures for supplier relationship management				x	
			4.6.2.2.b	Policies and procedures for customer-side relationship management					x
			4.6.2.2.c	Policies and procedures for contract management			partial (quick wins)	full	
		Financial Management for SAM	4.6.3.2.a	Definition of financial information required				x	
			4.6.3.2.b	Budgets				x	
			4.6.3.2.c	Reporting of actual against budget				x	
			4.6.3.2.d	Availability of asset value information				x	
			4.6.3.2.e	Reviews of actual against budget and follow-up				x	
			4.6.3.2.f	License optimization			partial (quick wins)	full	
		Service Level Management for SAM	4.6.4.2.a	Definition of service level agreements				x	
			4.6.4.2.b	Reporting of actuals against targets				x	
			4.6.4.2.c	Reviews of performance				x	
		Security Management for SAM	4.6.5.2.a	Security policy for SAM resources					x
			4.6.5.2.b	Specification of access controls for SAM resources					x
			4.6.5.2.c	Execution of access controls					x

Major Name	Minor Name	Process Area Name	Outcome	Caption	Additional Comments	Tier 1	Tier 2	Tier 3	Tier 4
Primary Process Interfaces for SAM	Life Cycle Process Interfaces for SAM	Change Management Process	4.7.2.2.a	Change management process definition					x
		Acquisition Process	4.7.3.2.a	Standard architectures				x	
			4.7.3.2.b	Standard configurations				x	
			4.7.3.2.c	Procurement policies and procedures				x	
			4.7.3.2.d	Policies and procedures for receipt processing				x	
		Software Development Process	4.7.4.2.a	Software development process definition for consideration of SAM requirements					x
			4.7.4.2.b	Software development process definition for asset control					x
		Software Release Management Process	4.7.5.2.a	Software release management process definition					x
		Software Deployment Process	4.7.6.2.a	Software deployment process definition				x	
		Incident Management Process	4.7.7.2.a	Incident management process definition					x
		Problem Management Process	4.7.8.2.a	Problem management process definition					x
		Retirement Process	4.7.9.2.a	Retirement process definition				x	

Key: ‘x’ – indicates tier includes all subclauses of this outcome; ‘partial’ – selected subclauses of this outcome included in tier (see normative clause for selections).

Annex B
(informative)

Guidance on selected topics

B.1 Introduction

This Annex provides guidance on selected topics relevant to this part of ISO/IEC 19770. Further industry guidance is also available, such as described in *Annex C*.

B.2 Releases

The term *release* will often apply to a final *internal production release*, for example, the release of a distribution copy which has been technically approved, or a corporate build which is then released for use with certain devices e.g. on a quantity of desktop computers.

A second usage variant of the terms *release* and *build* applies to software assets within the software development process. These terms are also in common use in the consumption of Open Source Software e.g. a *release* of OSS code to users who may then *build* this software themselves. This part of ISO/IEC 19770 does not define development-type processes but makes provision for assets to be identified and controlled, leaving freedom to apply SAM processes which could equally be applied to software assets in either of the two usage contexts above. (See *1.2 Field of application* for a discussion of the applicability of this part of ISO/IEC 19770 to development.)

Whilst any release may be managed using this part of ISO/IEC 19770 it is recognized that where the term release appears twice in a sequence of events this may need further explanation, especially given that formal approval may be required for *both* releases. To give a combined example, a corporate build process may be made up of more than one successive step combining manufactured software with builds of released code from internal developers and may include a source-code release from OSS development. This process will typically include patches. Some or all of these activities are sometimes referred to as packaging. Packaging usually implies the addition of a software 'wrapper' that is required by a specific software deployment utility.

Several such corporate builds are usually tested and technically approved before a distribution copy (sometimes in the form of an image) is created and approved for final release to the live environment.

In conclusion, this part of ISO/IEC 19770 can be used to manage both kinds of released software assets - the code release by developers and the internal production release from successive packaging activities. Both may be in-scope, covered by inventory processes and record verifications and any release being managed must be technically approved and then finally be authorized for deployment, with an authorized inventory of installs.

B.3 Document and record management

There is no explicit requirement for document and record management in this part of ISO/IEC 19770, but nonetheless this is effectively required such as in:

a) 4.2.4.2 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.");

b) 4.2.4.2 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) 4.5.5.2 b) (“Documentary evidence exists that demonstrates (a) that the verification procedures above are being performed, and (b) that corrective follow-up action is taken until successful completion on the causes of all identified exceptions.”)

It is strongly recommended that organizations implementing this part of ISO/IEC 19770 should also implement document and record management as required for Management System Standards such as ISO 9001:2000 and ISO/IEC 20000-1:2005, and this will provide the necessary general capabilities required.

Annex C
(informative)

Cross reference to industry best practice guidance

C.1 Introduction

As explained in 1.1, this part of ISO/IEC 19770 does not detail SAM processes in terms of methods or procedures required to meet the requirements for outcomes of a process. Likewise, 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.

Although this part of ISO/IEC 19770 does not detail these topics, nonetheless these topics are of major importance in being able to implement SAM and meet the requirements of this part of ISO/IEC 19770. This part of ISO/IEC 19770 does not endorse any specific source of guidance on SAM and no ISO/IEC endorsement of related products or the sourcing organizations is implied. However, it is relevant to indicate that sources of guidance do exist to which reference may be made as examples.

C.2 Sources

As of the writing of this part of ISO/IEC 19770, there are at least three major sources of such guidance on SAM, all of which are represented by individuals in the Working Group responsible for this part of ISO/IEC 19770. These are examples only. The public review process associated with the development of this part of ISO/IEC 19770 identified several others, namely CMMI, FFIEC, BSA SAM Advantage, Gartner, Institute for Technology Asset Management and ISEB SAM Essentials. Furthermore, there are others available (subsequently cited by a National Body) such as Agnitio Advisor's [http://www.agnitioadvisors.com/Assessment] and IBSMA guides [http://www.ecpmedia.com/publications.html#sm_guidetosam].

The three major sources for guidance on SAM mentioned above, in order of publication, are:

- ITIL® V3 Guide to Software Asset Management, TSO, © 2009, ISBN 978 0 11 331106 4. Version 2 of this publication was developed before ISO/IEC 19770-1:2006 was developed. In many respects it was the predecessor of ISO/IEC 19770-1:2006.

- IAITAM Best Practice Library, International Association of IT Asset Managers, [www.iaitam.org] ©2008, ISBN 978-1-935019-00-8, 978-1-935019-01-5, 978-1-935019-02-2, 978-1-935019-03-9, 978-1-935019-04-6, 978-1-935019-05-3, 978-1-935019-06-0, 978-1-935019-07-7, 978-1-935019-08-4, 978-1-935019-09-1, 978-1-935019-10-7, 978-1-935019-11-4. This best practice guidance is a quite comprehensive 12 volume set, and covers all of IT Asset Management, not just Software Asset Management. It was developed before ISO/IEC 19770-1:2006 was published. This ISO/IEC document references IBPL, used by permission of IAITAM. ©2008 IAITAM. All rights reserved.

- SAM Standard and Evaluation Criteria, SAMAC, [www.samac.or.jp] Software Asset Management Standard, the association of SAM Assessment and Certification, Japan ©2010. This documentation is in Japanese and English. Although it is titled a standard, it is primarily best practice. It was revised after ISO/IEC 19770-1:2006 was published, and is aligned to ISO/IEC 19770-1:2006. This ISO/IEC document references the SAMAC standard v2, used by permission of the SAMAC. © SAMAC 2010. All rights reserved.

In order to facilitate access to this guidance, the table at the end of this annex gives mappings from this part of ISO/IEC 19770-1 to the last two of the sources cited above.

This ISO/IEC document also includes CobiT 4.1®, used by permission of ISACA/ITGI [www.isaca.org]. ©1996-2007 ITGI. All rights reserved. CobiT is a set of tools and techniques for controlling and managing IT. It forms a framework for IT governance helping managers set objectives for IT departments that in-turn support business objectives.

C.3 Further information on CobiT selected mappings

Introducing best practices, both in the case of CobiT and this part of ISO/IEC 19770 or indeed any other IT management framework, takes time and requires many steps. Tiers enable selective targeting of immediate improvement and identify areas for later attention. A supporting approach may use CobiT but connected objectives are defined differently, so the following guidance shows some of the connections. It may be used by organizations who already use CobiT, providing an indication of which CobiT processes support each tier. (Completion of all CobiT connections does not imply conformance to the requirements of Tier 1 of this part of 19770.)

As with all Annexes to this part of 19770, this content is informative of the relating themes found in other practices and assessments. It is intended as a guide only and not as a definitive interpretation of CobiT knowledge. See also *Annex E* for further information about how CobiT relates to other available methodologies.

C.3.1 About mapping Tier 1 trustworthy data to CobiT

Achieving this means knowing what you have so that you can manage it.

Organizations achieving Tier 1 rely on management activities for the collection and verification of knowledge about IT assets and their status. It is especially supported by configuration management disciplines. In CobiT these activities are related to managing and monitoring the information about IT infrastructure, resources and capabilities, information architecture, and other assets.

In particular the following CobiT processes support achieving the Tier 1 outcomes:

CobiT Process	Comment
DS11 Manage Data	The requirements for this process include establishing procedures and identifying requirements for managing the SAM data
PO2 Define the information architecture.	The definition of the Information Architecture establishes a solid base for managing the IT asset data
ME1 Monitor and Evaluate IT Performance	The requirements for monitoring inventory and verification processes to ensure data is controlled
DS9 Manage the Configuration	The CI information collected in this process includes significant amount of data to be managed in SAM.

C.3.2 About mapping Tier 2 practical management to CobiT

Achieving this means improving management controls and driving immediate benefits.

In this tier the activities are known as Management, Control and Governance activities. The outcomes to be achieved here require the introduction of pro-active management together with attention to the planning of SAM itself. It also requires control over the SAM processes now implemented, including monitoring and verification of their outcomes. In CobiT related processes are grouped and referred to as “Plan and Organize” and “Monitor and Evaluate”.

In particular the following CobiT processes support achieving the Tier 2 outcomes:

CobiT Process	Comment
PO4 Define the IT processes, organization and relationships.	The requirements for PO4 build the foundation for the SAM control environment
ME3 Ensure compliance with external requirements	Legislation and regulatory requirements are addressed as part of Tier 2 control environment. (License compliance actions are decided in Tier 1)
ME4 Provide IT Governance	Governance establishment provides definitions for management and control
PO5 Manage the IT investment.	Covers some of the outcomes of the Financial Management required in this tier
PO8 Manage quality	Quality Management System supports and defines the management activities
PO9 Assess and manage IT risks	Risk management is required in this tier
DS7 – Educate and train users	Aligns closely with Tier 2 Policies, procedures and procedures (especially communication of) for use of software assets.

C.3.3 About mapping Tier 3 operational integration to CobiT

Achieving this means improving efficiency and effectiveness.

In this tier the SAM processes integrate with the IT operation. Lifecycle of the Software and related assets is managed. Controls are established here to conform to the standards and external requirements. In CobiT, the lifecycle processes are defined mainly in the Acquire and Implement part and compliance is covered mainly in Deliver and Support processes.

In particular the following CobiT processes help achieving the Tier 3 outcomes:

CobiT Process	Comment
AI3 Acquire and Maintain Technology Infrastructure	Supports the lifecycle management of the technology that underpins the software
AI2 Acquire and Maintain Application software	Supports the lifecycle of software applications
AI5 Procure IT resources	Procurement procedures are defined and managed
DS1 Define and manage service levels	Direct relationship with Service Level Management requirements
DS2 Manage third-party services	Helps in managing the suppliers
DS6 Identify and allocate costs	Complete financial management is required in this tier
ME2 Monitor and evaluate internal control	Critical for proper financial management
DS3 – Manage performance and capacity	Supports service level management for SAM.

C.3.4 About mapping Tier 4 full ISO/IEC SAM conformance to CobiT

Achieving this means achieving best-in-class strategic SAM.

The last tier completes the objectives for SAM to support the business in its strategic goals. Thus IT Service management processes are now fully supported. SAM also acquires processes that ensure its stability and its own continual improvement. As a result, SAM is a complete system of processes the organization can rely on.

In CobiT, the strategic processes are spread around the whole framework providing guidance for making the specific IT management elements focused on being the best in class.

The following CobiT processes are identified as the most helpful in achieving the best possible strategic SAM:

CobiT Process	Comment
PO1 Define a Strategic IT Plan *See also the general CobiT: PO6 communicate management objectives. Stakeholders thus support the SAM objectives approved by the board in Tier 4.	Establish processes in strategic planning helps achieve business and IT alignment and integration. Tier 4 also includes approval* of SAM management objectives for SAM (4.2.2.2.e).
AI6 Manage Changes	Supports Tier 4 Change Management Process
AI7 Install and accredit solutions and changes	Required as part of change management
DS4 Ensure continuous service	Continuity of operations is required in this tier
DS5 Ensure systems security	Security management is required in this tier
DS8 Manage Service Desk and Incidents	This tier requires managing the customer feedback as well as the incident management process
DS10 Manage problems	Problem management process is required explicitly in this tier
ME1 Monitor and evaluate IT performance	Continual improvement is required in this tier.

Most connections in the above table show where a single CobiT process connect strongly to one tier. Some tiers, especially Tier 4 are also supported by one or more generalized CobiT processes. These offer indirect support for the ISO objectives, of broad support over one or more tiers. An example of such a general CobiT process would be DS13 Manage Operations, which indirectly supports Tier 3 Service Level Management and, in Tier 4, also supports Monitoring and Review of SAM, Continual Improvement and Software Asset Control.

C.3.5 Other CobiT processes

In addition to those processes listed above which directly support a specific tier, there are also other CobiT processes supporting SAM, either indirectly or generally. The following list of other CobiT processes is placed here for reference:

PO3 – Determine technological direction

PO6 – Communicate management aims and direction

PO7 – Manage IT Human Resources

PO10 – Manage Projects

AI1 – Identify automated solutions

AI4 – Enable operation and use

DS12 – Manage the physical environment

DS13 – Manage operations.

C.4 Cross reference table of outcomes to industry guidance

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
4.2 Control Environment for SAM The objective of the Control Environment for SAM is to establish and maintain the management system within which the other SAM processes are implemented.					
4.2.2 Corporate Governance Process for SAM 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 corporate board or equivalent body, and that appropriate mechanisms are in place to ensure the proper discharge of this responsibility.					
Implementation of the Corporate governance process for SAM will enable the organization to demonstrate that:	4.2.2.2				
There is a clear corporate statement for the purposes of this part of ISO/IEC 19770 about:	4.2.2.2.a	Tier 2	Program Management	1. Policy: Establishment of Policy and Regulation	ME4 Provide IT governance
the legal entity or parts of a legal entity which are included in scope.	4.2.2.2.a1	Tier 2	Project Management	1. Policy	PO4 Define the IT Processes, Organization and Relationships PO6 Communicate Management Aims and Direction ME4 Provide IT governance
the specific single body or individual that has overall corporate management responsibility for that entity or parts of that entity.	4.2.2.2.a2	Tier 2	Project Management	1. Policy	PO4 Define the IT Processes, Organization and Relationships, ME4 Provide IT governance
Responsibility for corporate governance of software and related assets is formally recognized by the corporate board or equivalent body.	4.2.2.2.b	Tier 2	Program Management	1. Policy	PO1 Define a Strategic IT Plan PO4.2 IT Strategy Committee PO10.3 Project Management Approach PO10.6 Project Phase Initiation PO10.11 Project Change Control ME4 Provide IT governance
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.	4.2.2.2.c	Tier 2	Policy Management	1. Policy	PO2 Define the Information Architecture ME3 Ensure compliance with external requirements
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:	4.2.2.2.d	Tier 2	Compliance Management	1. Policy	PO9 Assess and Manage IT Risks
Risk of regulatory non-compliance;	4.2.2.2.d1	Tier 2	Program Management Compliance Management Legislation Management	1. Policy	PO9 Assess and Manage IT Risks
Risk of violation of security requirements.	4.2.2.2.d2	Tier 2		1. Policy	PO9 Assess and Manage IT Risks DS5 Ensure Systems Security
Risk of licensing non-compliance	4.2.2.2.d3	Tier 2	Program Management Compliance Management Acquisition Management	1. Policy	PO9 Assess and Manage IT Risks ME3 Ensure compliance with external requirements AI2 Acquire and maintain application software

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
Risk of interruption of operations due to problems with the IT infrastructure which could result from inadequate SAM.	4.2.2.2.d4	Tier 2	Program Management Acquisition Management Asset Id Management Project Management	1. Policy	PO2 Define the Information Architecture PO9 Assess and Manage IT Risks
Risk of excessive spending on licensing and other IT support costs due to inadequate SAM.	4.2.2.2.d5	Tier 2	Program Management Acquisition Management Asset ID Management Financial Management Disposal Management	1. Policy	PO5 Manage the IT Investment AI1 Identify Automated Solutions DS6 Identify and Allocate Costs DS9 Manage the Configuration
Risks associated with decentralized vs. centralized management approaches for software and related assets.	4.2.2.2.d6	Tier 2	Program Management Acquisition Management Asset ID Management Disposal Management	1. Policy	PO9 Assess and Manage IT Risks
Risks associated with different countries of operation taking into account local compliance cultures and enforcement approaches.	4.2.2.2.d7	Tier 2	Program Management Compliance Management Legislation Management	1. Policy	ME3 Ensure compliance with external requirements PO4 Define the IT Processes, Organization and Relationships PO9 Assess and Manage IT Risks
The management objectives for SAM are approved by the corporate board or equivalent body, and reviewed at least annually.	4.2.2.2.e	Tier 4	Program Management	1. Policy	PO1 Define a Strategic IT Plan ME4 Provide IT governance ME2 Monitor and evaluate internal control
4.2.3 Roles and responsibility for SAM The objective of the roles and responsibilities for SAM process is to ensure that the roles and responsibilities for the software and related assets are clearly defined, maintained and understood by all personnel potentially affected.					
Implementation of the Roles and responsibilities for SAM Process will enable the organization to demonstrate that:	4.2.3.2		Program Management		PO4.6 Establishment of Roles and Responsibilities ME4 Provide IT governance
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:	4.2.3.2.a	Tier 2		2.Systems: Establishment of a Managerial System	PO4.6 Establishment of Roles and Responsibilities
Proposing management objectives for SAM	4.2.3.2.a1	Tier 2	Program Management	2.Systems	PO4.6 Establishment of Roles and Responsibilities
Overseeing the development of the SAM plan	4.2.3.2.a2	Tier 2	Program Management	2.Systems	PO4.6 Establishment of Roles and Responsibilities
Obtaining resources for implementing the approved SAM plan	4.2.3.2.a3	Tier 2	Program Management	2.Systems	PO4.10 Supervision
Delivering results against the SAM plan	4.2.3.2.a4	Tier 2	Program Management	2.Systems	PO4.6 Establishment of Roles and Responsibilities

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
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.	4.2.3.2.a5	Tier 2	Program Management	2.Systems	PO4.6 Establishment of Roles and Responsibilities
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:	4.2.3.2.b	Tier 2	Program Management	2.Systems	PO4.6 Establishment of Roles and Responsibilities
Obtaining resources for implementing the SAM plan.	4.2.3.2.b1	Tier 2	Program Management	2.Systems	PO4 Define the IT Processes, Organization and Relationships
Delivering results against the SAM plan.	4.2.3.2.b2	Tier 2	Program Management	2.Systems	PO4 Define the IT Processes, Organization and Relationships
Adopting and implementing necessary policies, processes and procedures.	4.2.3.2.b3	Tier 2	Program Management Policy Management	2.Systems	PO6 Communicate Management Aims and Direction
Maintaining accurate records of software and related assets.	4.2.3.2.b4	Tier 2	Program Management	2.Systems	PO1.4 IT Strategic Plan
Ensuring that management and technical approvals are required for procurement, deployment and control of software assets.	4.2.3.2.b5	Tier 2	Acquisition Management	2.Systems	PO10.8 Project Resources
Managing contracts, supplier relationships, and internal customer relationships	4.2.3.2.b6	Tier 2	Program Management Documentation Management Vendor Management	2.Systems	PO4 Define the IT Processes, Organization and Relationships PO8.4 Customer Focus PO10 Manage Projects DS1.6 Review of Service Level Agreements and Contracts
Identifying the need for and implementing improvements	4.2.3.2.b7	Tier 2	Program Management	2.Systems	DS10.4 Integration of Configuration, Incident and Problem Management
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.	4.2.3.2.c	Tier 2	Communication & Education Management	2.Systems	PO4.6 Establishment of Roles and Responsibilities
4.2.4 Policies, processes and procedures for SAM 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					
Implementation of the Policies, processes and procedures for SAM process will enable the organization to demonstrate that:	4.2.4.2				PO4 Define the IT Processes, Organization and Relationships
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.	4.2.4.2.a	Tier 2	Policy Management	1. Policy	PO2 Define the Information Architecture ME2 Monitor and evaluate internal control PO3 Determine Technological Direction

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
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.	4.2.4.2.b	Tier 2	Policy Management	1. Policy	PO2 Define the Information Architecture PO2.1 Enterprise Information Architecture PO2.3 Data Classification Scheme
Policies are developed, approved and issued covering at a minimum:	4.2.4.2.c	Tier 2	Policy Management Communication & Education Management	1. Policy	PO1 Define a Strategic IT Plan PO2 Define the Information Architecture PO6 Communicate Management Aims and Direction PO8 Manage Quality DS7 Educate and train users
Individual and corporate responsibilities for corporate governance of software and related assets.	4.2.4.2.c1	Tier 2	Policy Management Program Management	1. Policy	PO1 Define a Strategic IT Plan PO2 Define the Information Architecture PO4 Define the IT Processes, Organization and Relationships PO4.6 Establishment of Roles and Responsibilities PO4.7 Responsibility for IT Quality Assurance
Any restrictions on personal use of corporate software and related assets.	4.2.4.2.c2	Tier 2	Policy Management	1. Policy	PO4.8 Responsibility for Risk, Security and Compliance
Requirement for compliance with legal and regulatory requirements, including for copyright and data protection.	4.2.4.2.c3	Tier 2	Compliance Management Policy Management	1. Policy	ME3 Ensure compliance with external requirements PO4.8 Responsibility for Risk, Security and Compliance
Any procurement requirements (e.g. use of corporate agreements, or buying only from reputable/approved suppliers)	4.2.4.2.c4	Tier 2	Acquisition Management Policy Management	1. Policy	AI1 Identify Automated Solutions PO4.8 Responsibility for Risk, Security and Compliance
Any requirement for approvals for installation or use of software, whether purchased or not.	4.2.4.2.c5	Tier 2	Acquisition Management	1. Policy	PO2 Define the Information Architecture PO10 Manage Projects
Disciplinary implications of violation of these policies.	4.2.4.2.c6	Tier 2	Policy Management	1. Policy	ME2 Monitor and evaluate internal control DS5 Ensure Systems Security
Policies and procedures are communicated to all personnel in a way which (a) reaches all new personnel when they start, and continuing personnel at least annually; (b) requires positive acknowledgement back from personnel when they start and at least annually; and (c) is readily accessible at all times to personnel.	4.2.4.2.d	Tier 2	Communication & Education Management	1. Policy 3. Competence: Establishment and Maintenance of Competence in SAM 5. Implement'n: Confirmation of Software and Related Asset Implemented	DS7 Educate and train users PO1 Define a Strategic IT Plan PO2 Define the Information Architecture PO6 Communicate Management Aims and Direction PO8 Manage Quality

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
4.2.5 Competence in SAM The objective of the Competence in SAM process is to ensure that appropriate competence and expertise in SAM is available and is being applied.					
Implementation of the Competence in SAM process will enable the organization to Demonstrate that:	4.2.5.2				PO6 Communicate Management Aims and Direction PO7 Manage IT Human Resources
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:	4.2.5.2.a	Tier 2	Communication & Education Management	3.Competence	PO7 Manage IT Human Resources
SAM in general.	4.2.5.2.a1	Tier 2	Communication & Education Management	3.Competence	PO7 Manage IT Human Resources
Licensing for software manufacturers whose software is being used.	4.2.5.2.a2	Tier 2	Communication & Education Management	3.Competence	AI5 Procure IT Resources AI6 Manage Changes DS9 Manage the Configuration DS9.3 Configuration Integrity Review DS9.3 Configuration Integrity Review
A review is undertaken at least annually to determine what constitutes "Proof of License" for the software manufacturer.	4.2.5.2.b	Tier 4	Compliance Management	3.Competence	ME2 Monitor and evaluate internal control AI6 Manage Changes DS9 Manage the Configuration DS9.3 Configuration Integrity Review
Personnel with SAM management responsibilities receive training in SAM and in relevant licensing, including both initial training and formal continuing education annually.	4.2.5.2.c	Tier 2	Communication & Education Management	3.Competence	PO7 Manage IT Human Resources
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	4.2.5.2.d	Tier 2	Compliance Management	3.Competence	PO1 Define a Strategic IT Plan PO2 Define the Information Architecture PO3 Determine Technological Direction PO3.4 Technology Standards PO3.5 IT Architecture Board PO4 Define the IT Processes, Organization and Relationships PO4.1 IT Process Framework Define an IT process PO4.8 Responsibility for Risk, Security and Compliance PO6 Communicate Management Aims and Direction PO8.6 Quality Measurement, Monitoring and Review

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
4.3 Planning and Implementation Processes for SAM The objective of Planning and implementation processes for SAM is to ensure the effective and efficient accomplishment of SAM management objectives.					
4.3.2 Planning for SAM The objective of the Planning for SAM process is to ensure appropriate preparation and planning for the effective and efficient accomplishment of SAM objectives.					
Implementation of the Planning for SAM process will enable the organization to demonstrate that:	4.3.2.2				PO1 Define a Strategic IT Plan PO3 Determine Technological Direction P010 Manage projects
Management objectives for SAM are developed and proposed for approval by the corporate board or equivalent body, and updated at least annually	4.3.2.2.a	Tier 4	Program Management	1. Policy	PO4.8 Responsibility for Risk, Security and Compliance PO5 Manage the IT Investment PO9.6 Maintenance and Monitoring of a Risk Action Plan AI1 Identify Automated Solutions PO6 Communicate Management Aims and Direction ME4 Provide IT governance
A plan (the 'SAM plan') for implementing and delivering SAM is developed and documented, and updated at least annually, which includes:	4.3.2.2.b	Tier 2	Program Management	1. Policy	PO4.8 Responsibility for Risk, Security and Compliance PO5 Manage the IT Investment PO9.6 Maintenance and Monitoring of a Risk Action Plan AI1 Identify Automated Solutions PO1 Define a Strategic IT Plan
A clear scope statement ('software asset scope') describing which types of software are included; the coverage of related assets, including any beyond the minimum required by this part of ISO/IEC 19770; and any interfaces with or requirements for other organizations or systems.	4.3.2.2.b1	Tier 2	Program Management Compliance Management	1. Policy	AI1 Identify Automated Solutions DS9 Manage the Configuration
A clear specification of which policies, processes and procedures are required for assets in scope.	4.3.2.2.b2	Tier 2	Program Management Policy Management Acquisition Management	1. Policy	PO6 Communicate Management Aims and Direction P07 Manage IT human resources
A clear explanation of the approach to managing, auditing and improving SAM including automation as appropriate to support the processes.	4.3.2.2.b3	Tier 2	Program Management	1. Policy	PO2 Define the Information Architecture PO3 Determine Technological Direction PO8.3 Development and Acquisition Standards AI1 Identify Automated Solutions
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.	4.3.2.2.b4	Tier 2	Program Management Compliance Management Legislation Management	1. Policy	PO2 Define the Information Architecture PO3 Determine Technological Direction PO8.3 Development and Acquisition Standards AI1 Identify Automated Solutions DS8 Manage service desk and incidents DS10 Manage Problems
Schedules and responsibilities for periodic activities, including preparation of management reports and performance of verification and compliance activities.	4.3.2.2.b5	Tier 2	Program Management	1. Policy	PO2 Define the Information Architecture PO3 Determine Technological Direction PO8.3 Development and Acquisition Standards AI1 Identify Automated Solutions ME1 Monitor and evaluate IT performance

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
Identification of the resources including budget needed to implement the SAM plan.	4.3.2.2.b6	Tier 2	Program Management	1. Policy	PO2 Define the Information Architecture PO3 Determine Technological Direction PO8.3 Development and Acquisition Standards AI1 Identify Automated Solutions PO5 Manage the IT Investment, DS6 Identify and Allocate Costs
Performance measures for tracking accomplishment against the SAM plan, including target measures for accuracy of the asset management records.	4.3.2.2.b7	Tier 2	Program Management Compliance Management	1. Policy	PO2 Define the Information Architecture PO3 Determine Technological Direction PO8.3 Development and Acquisition Standards AI1 Identify Automated Solutions ME1 Monitor and evaluate IT performance
The plan is approved by the corporate board or equivalent body	4.3.2.2.c	Tier 2	Program Management	1. Policy	PO4.8 Responsibility for Risk, Security and Compliance PO5 Manage the IT Investment PO9.6 Maintenance and Monitoring of a Risk Action Plan ME4 Provide IT governance
4.3.3 Implementation of SAM The objective of the Implementation of SAM process is to accomplish overall SAM objectives and the SAM plan.					
Implementation of the Implementation of SAM process will enable the organization to demonstrate that:	4.3.3.2				
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	4.3.3.2.a	Tier 4	Program Management Communication & Education Management	2. Systems	AI6 Manage Changes PO9 Assess and Manage IT Risks PO6 Communicate Management Aims and Direction
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.	4.3.3.2.b	Tier 4	Program Management Communication & Education Management	2. Systems	ME2 Monitor and evaluate internal control PO6 Communicate Management Aims and Direction
Follow-up on any variances identified takes place promptly and is documented.	4.3.3.2.c	Tier 4	Program Management	2. Systems	ME1 Monitor and evaluate IT performance ME2 Monitor and evaluate internal control ME3 Ensure compliance with external requirements ME4 Provide IT governance PO6 Communicate Management Aims and Direction PO7 Manage IT Human Resources

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
4.3.4 Monitoring and review of SAM The objective of the Monitoring and review of SAM process is to ensure that the management objectives for SAM are being achieved					
Implementation of the Monitoring and review of SAM process will enable the organization to demonstrate that:	4.3.4.2				ME1 Monitor and evaluate IT performance
A formal review is conducted at least annually:	4.3.4.2.a	Tier 4	Program Management	3. Competence 4. Ownership: Confirmation and Verification of Licenses Owned 5. Implement'n	ME1 Monitor and evaluate IT performance
to assess whether management objectives for SAM and the SAM plan are being achieved	4.3.4.2.a1	Tier 4	Program Management	3. Competence 4. Ownership 5. Implement'n	ME1 Monitor and evaluate IT performance
to summarize performance against all performance measures specified in the SAM plan and in service level agreements related to SAM	4.3.4.2.a2	Tier 4	Program Management	3. Competence 4. Ownership 5. Implement'n	ME2 Monitor and evaluate internal control PO8 Manage Quality
to provide a summary of the findings of the Conformance verification for SAM process	4.3.4.2.a3	Tier 4	Compliance Management	3. Competence 4. Ownership 5. Implement'n	PO8 Manage Quality ME3 Ensure compliance with external requirements
to conclude on the basis of the above whether:	4.3.4.2.a4	Tier 4		3. Competence 4. Ownership 5. Implement'n	
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	4.3.4.2.a4i	Tier 4	Policy Management Communication & Education Management	3. Competence 4. Ownership 5. Implement'n	PO1 Define a Strategic IT Plan PO2.4 Integrity Management PO4 Define the IT Processes, Organization and Relationships PO4.14 Contracted Staff Policies and Procedures
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	4.3.4.2.a4ii	Tier 4	Program Management Compliance Management	3. Competence 4. Ownership 5. Implement'n	PO1 Define a Strategic IT Plan PO2.4 Integrity Management PO4 Define the IT Processes, Organization and Relationships PO4.14 Contracted Staff Policies and Procedures
to summarize any exceptions identified and actions which may need to be taken as a result of the above	4.3.4.2.a5	Tier 4	Program Management	3. Competence 4. Ownership 5. Implement'n	PO1 Define a Strategic IT Plan PO2.4 Integrity Management PO4 Define the IT Processes, Organization and Relationships PO4.14 Contracted Staff Policies and Procedures
to identify opportunities for improvement in the provision of services for software and related assets	4.3.4.2.a6	Tier 4	Program Management	3. Competence 4. Ownership 5. Implement'n	PO1 Define a Strategic IT Plan PO1.1 IT Value Management PO1.3 Assessment of Current Capability and Performance PO1.4 IT Strategic Plan PO1.5 IT Tactical Plans PO3 Determine Technological Direction PO4.3 IT Steering Committee PO4 Define the IT Processes, Organization and Relationships
to consider whether there is a need for a review of policies, processes and procedures as to their continued appropriateness, completeness and correctness.	4.3.4.2.a7	Tier 4	Policy Management	3. Competence 4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
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.	4.3.4.2.b	Tier 4	Program Management	3. Competence 4. Ownership 5. Implement'n	PO2 Define the Information Architecture
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.	4.3.4.2.c	Tier 4	Program Management	3. Competence 4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration
4.3.5 Continual Improvement of SAM 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.					
Implementation of the Continual improvement of SAM process will enable the organization to demonstrate that:	4.3.5.2				PO2 Define the Information Architecture PO4.1 IT Process Framework
A mechanism is in place to collect and record suggested improvements in SAM arising from all sources throughout the year.	4.3.5.2.a	Tier 4	Communication & Education Management	2. Systems 4. Ownership	PO2 Define the Information Architecture PO4.1 IT Process Framework
Suggestions for improvement are periodically assessed, prioritized and approved for incorporation in SAM implementation and improvement plans.	4.3.5.2.b	Tier 4	Program Management	2. Systems 4. Ownership	PO2 Define the Information Architecture PO4.1 IT Process Framework
4.4 Inventory Processes for SAM The objective of Inventory processes for SAM is to create and maintain all stores and records for software and related assets, and to 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 project encompassing all of IT service management, Inventory processes for SAM would be considered part of configuration management.					
4.4.2 Software Asset Identification 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.					
Implementation of the Software asset identification process will enable the organization to demonstrate that:	4.4.2.2				PO2 Define the Information Architecture PO4.1 IT Process Framework DS9 Manage the Configuration
Types of assets to be controlled and the information associated with them are formally defined, taking into account the following:	4.4.2.2.a	Tier 4		1. Policy 4. Ownership 5. Implement'n	PO2 Define the Information Architecture AI1 Identify Automated Solutions PO1.5 IT Tactical Plans PO5 Manage the IT Investment PO9 Assess and Manage IT Risks
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.	4.4.2.2.a1	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS5 Ensure Systems Security DS9.1 Configuration Repository and Baseline
Items to be managed include:	4.4.2.2.a2	Tier 4		1. Policy 4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks
All platforms on which software can be installed or run	4.4.2.2.a2i	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks PO10 Manage Projects DS9 Manage the Configuration
Software definitive master versions and distribution copies	4.4.2.2.a2ii	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
Software builds and releases (originals and distribution copies)	4.4.2.2.a2iii	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration
All installed software	4.4.2.2.a2iv	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	PO10 Manage Projects DS9 Manage the Configuration
Software versions	4.4.2.2.a2v	Tier 4	Asset Identification Management Program Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration
Methodology by which software within scope is identified	4.4.2.2.a2vi	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	PO10 Manage Projects DS9 Manage the Configuration
Patches and updates	4.4.2.2.a2vii	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration
Licenses including underlying licenses and effective full licenses	4.4.2.2.a2viii	Tier 4	Asset Identification Management Compliance Management	1. Policy 4. Ownership 5. Implement'n	AI2 Acquire and maintain application software
Proof of license documentation	4.4.2.2.a2ix	Tier 4	Compliance Management Documentation Management	1. Policy 4. Ownership 5. Implement'n	AI2 Acquire and maintain application software
Contracts (including terms and conditions) relating to software assets, including both hard-copy and electronic	4.4.2.2.a2x	Tier 4	Compliance Management Documentation Management Acquisition Management	1. Policy 4. Ownership 5. Implement'n	AI2 Acquire and maintain application software
Both physical and electronic stores of the above, as relevant	4.4.2.2.a2xi	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration
Licensing models	4.4.2.2.a2xii	Tier 4	Compliance Management	1. Policy 4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks PO5 Manage the IT Investment
Software shall be manageable both by files and by packages corresponding to specific products released by software manufacturers or developers.	4.4.2.2.a3	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS12 Manage the Physical Environment
Basic information required for all assets is	4.4.2.2.a4	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration
Unique identifier	4.4.2.2.a4i	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration
Name/description	4.4.2.2.a4ii	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration
Location	4.4.2.2.a4iii	Tier 4	Asset Identification Management Program Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
Custodianship (or owner)	4.4.2.2.a4iv	Tier 4	Asset Identification Management Program Management Acquisition Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration
Status (e.g. test/production status; development or build status)	4.4.2.2.a4v	Tier 4	Asset Identification Management Program Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration
Type (e.g. software, hardware, facility)	4.4.2.2.a4vi	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration
Version (where applicable)	4.4.2.2.a4vii	Tier 4	Asset Identification Management	1. Policy 4. Ownership 5. Implement'n	DS9 Manage the Configuration
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.	4.4.2.2.b	Tier 1	Asset Identification Management Documentation Management	4. Ownership 5. Implement'n	DS9 Manage the Configuration DS12 Manage the Physical Environment
4.4.3 Software asset Inventory management 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.					
Implementation of the Software asset inventory management process will enable the organization to demonstrate that:	4.4.3.2				DS13.4 Sensitive Documents and Output Devices
Policies and procedures are developed, approved and issued which include the management and maintenance of inventories and physical/electronic stores including access controls which:	4.4.3.2.a	Tier 1	Policy Management Communication & Education Management	4. Ownership 5. Implement'n	DS9 Manage the Configuration , DS13.4 Sensitive Documents and Output Devices
protect them from unauthorized access, change or corruption.	4.4.3.2.a1	Tier 1	Policy Management	4. Ownership 5. Implement'n	PO7.8 Job Change and Termination DS5.3 Identity Management
provide a means for disaster recovery.	4.4.3.2.a2	Tier 1	Documentation Management	4. Ownership 5. Implement'n	DS4.1 IT Continuity Framework
Inventories exist of:	4.4.3.2.b	Tier 1		4. Ownership 5. Implement'n	
all platforms on which software assets can be installed or run.	4.4.3.2.b1	Tier 1	Asset Identification Management	4. Ownership 5. Implement'n	DS9 Manage the Configuration PO10 Manage Projects
all authorized installed software showing (a) packages and versions which can be	4.4.3.2.b2	Tier 1	Asset Identification Management	4. Ownership 5. Implement'n	DS9 Manage the Configuration PO10 Manage Projects
underlying licenses and effective full licenses held.	4.4.3.2.b3	Tier 1	Asset Identification Management Documentation Management	4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration
Inventories and corresponding physical/electronic stores exist of:	4.4.3.2.c	Tier 1	Asset Identification Management	4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration
software (definitive master versions and distribution copies)	4.4.3.2.c1	Tier 1	Asset Identification Management	4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
software builds and releases (originals and distribution copies)	4.4.3.2.c2	Tier 4	Asset Identification Management	4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration
contracts relating to software assets, both hard-copy and electronic	4.4.3.2.c3	Tier 1	Asset Identification Management Documentation Management	4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration
Proof of license documentation.	4.4.3.2.c4	Tier 1	Documentation Management	4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration PO5 Manage the IT Investment AI1 Identify Automated Solutions AI2 Acquire and maintain application software
Inventories or other clearly defined analysis or metric mechanisms exist to determine any licensing usage based on criteria other than software installations.	4.4.3.2.d	Tier 1	Asset Identification Management Program Management	5. Implement'n	PO9 Assess and Manage IT Risks PO10 Manage Projects
Arrangements are made to ensure the continued availability of the sources listed above.	4.4.3.2.e	Tier 4	Documentation Management	4. Ownership 5. Implement'n	PO5 Manage the IT Investment AI1 Identify Automated Solutions
Each inventory report produced has a clear description including its identity, purpose, and details of the data source.	4.4.3.2.f	Tier 4	Asset Identification Management	4. Ownership 5. Implement'n	PO5 Manage the IT Investment AI1 Identify Automated Solutions DS13.4 Sensitive Documents and Output Devices
4.4.4 Software Asset Control 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.					
Implementation of the Software asset control process will enable the organization to demonstrate that:	4.4.4.2				
An audit trail is maintained of changes made to software and related assets including changes in the status, location, custodianship and version	4.4.4.2.a	Tier 4	Asset Identification Management Program Management	4. Ownership 5. Implement'n	AI7 Install and Accredit Solutions and Changes AI7.5 System and Data Conversion DS9 Manage the Configuration
Policies and procedures are developed, approved and issued for the development, maintenance and management of software versions, images/builds and releases.	4.4.4.2.b	Tier 4	Policy Management Communication & Education Management	4. Ownership	PO1 Define a Strategic IT Plan PO2.4 Integrity Management PO4 Define the IT Processes, Organization and Relationships PO4.14 Contracted Staff Policies and Procedures DS9 Manage the Configuration
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.	4.4.4.2.c	Tier 4	Policy Management Communication & Education Management	4. Ownership	PO1 Define a Strategic IT Plan PO2.4 Integrity Management PO4 Define the IT Processes, Organization and Relationships PO4.14 Contracted Staff Policies and Procedures DS9 Manage the Configuration
4.5 Verification and Compliance Processes for SAM The objective of Verification and compliance processes for SAM is to 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 do not refer to audits conducted by software manufacturers, 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.					

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
4.5.2 Software Asset Record Verification 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.					
Implementation of the Software asset record verification process will enable the organization to demonstrate that:	4.5.2.2				PO1 Define a Strategic IT Plan PO1 Define a Strategic IT Plan PO3 Determine Technological Direction P010 Manage projects DS9 Manage the Configuration ME2 Monitor and evaluate internal control
Procedures are developed, approved and issued for the Software asset record verification process to include:	4.5.2.2.a	Tier 1	Program Management Compliance Management	4. Ownership 5. Implement'n	PO1 Define a Strategic IT Plan PO2.4 Integrity Management PO4 Define the IT Processes, Organization and Relationships PO4.14 Contracted Staff Policies and Procedures
Whenever scope is defined or changed, there is a validation of that scope by reviewing contract and purchase history in order to ensure the organizational and software scopes are aligned with business requirements.	4.5.2.2.a1	Tier 1	Program Management Compliance Management	4. Ownership 5. Implement'n	PO1 Define a Strategic IT Plan PO2.4 Integrity Management PO4 Define the IT Processes, Organization and Relationships PO4.14 Contracted Staff Policies and Procedures
At least quarterly there is reconciliation between what is installed on each platform and what was authorized for installation, including reporting on exceptions identified in what is currently installed, and in what has changed since the previous reconciliation.	4.5.2.2.a2	Tier 1	Program Management Compliance Management Asset Identification Management	4. Ownership 5. Implement'n	DS9 Manage the Configuration , ME2 Monitor and evaluate internal control PO9 Assess and Manage IT Risks PO10 Manage Projects
The hardware inventory including locations is verified at least 6-monthly, including reporting on exceptions identified.	4.5.2.2.a3	Tier 1	Program Management Compliance Management Asset Identification Management	4. Ownership 5. Implement'n	DS9 Manage the Configuration , ME2 Monitor and evaluate internal control PO5 Manage the IT Investment AI1 Identify Automated Solutions DS13.4 Sensitive Documents and Output Devices
The inventory of software programs (definitive master versions and distribution copies) is verified at least 6-monthly, including reporting on exceptions identified.	4.5.2.2.a4	Tier 4	Asset Identification Management	4. Ownership 5. Implement'n	AI2 Acquire and maintain application software DS9 Manage the Configuration ME2 Monitor and evaluate internal control PO5 Manage the IT Investment AI1 Identify Automated Solutions DS13.4 Sensitive Documents and Output Devices
The inventory of software builds (originals and distribution copies) is verified at least 6-monthly, including reporting on exceptions identified.	4.5.2.2.a5	Tier 4	Asset Identification Management	4. Ownership 5. Implement'n	AI2 Acquire and maintain application software DS9 Manage the Configuration ME2 Monitor and evaluate internal control
The physical store of proof of license documentation is verified (including for authenticity) at least annually, including reporting on exceptions identified.	4.5.2.2.a6	Tier 4	Documentation Management	4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration
The bases for and calculations of effective licenses from underlying licenses are reviewed at least annually, to ensure that necessary underlying licenses exist and that quantities are not being double-counted.	4.5.2.2.a7	Tier 4	Compliance Management Acquisition Management	4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
The physical store of contractual documentation related to software assets is verified for completeness at least annually, including reporting on exceptions identified.	4.5.2.2.a8	Tier 1	Documentation Management	4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration
The contracts inventory is verified at least annually, including reporting on exceptions identified.	4.5.2.2.a9	Tier 1	Documentation Management Asset Identification Management	4. Ownership 5. Implement'n	PO5 Manage the IT Investment AI1 Identify Automated Solutions DS13.4 Sensitive Documents and Output Devices PO5 Manage the IT Investment AI1 Identify Automated Solutions DS13.4 Sensitive Documents and Output Devices
There is a periodic review of historical invoices for the purpose of identifying incorrect billing and overpayment.	4.5.2.2.a10	Tier 2	Financial Management	4. Ownership 5. Implement'n	ME2 Monitor and evaluate internal control ME3 Ensure compliance with external requirements DS2 Manage Third-party Services
Follow-up corrective actions on any discrepancies or issues identified above take place and are documented	4.5.2.2.a11	Tier 1 – 4	Program Management	4. Ownership 5. Implement'n	DS5 Ensure Systems Security DS10 Manage Problems ME3.4 Positive Assurance of Compliance
4.5.3 Software Licensing Compliance The objective of the Software licensing compliance process is to ensure that all intellectual property used by the organization but owned by others, pertaining to software and related assets, is properly licensed and used in accordance with its terms and conditions.					
Implementation of the Software licensing compliance process will enable the organization to demonstrate that:	4.5.3.2				PO1 Define a Strategic IT Plan PO3 Determine Technological Direction P010 Manage projects
Procedures are developed, approved and issued for the Software licensing compliance process to include the following:	4.5.3.2.a	Tier 1		4. Ownership 5. Implement'n	PO1 Define a Strategic IT Plan PO2.4 Integrity Management PO4 Define the IT Processes, Organization and Relationships PO4.14 Contracted Staff Policies and Procedures
Reconciliation is conducted at least quarterly between effective licenses owned and licenses required for software used, taking into account the way licensing requirements are determined as per license terms and conditions.	4.5.3.2.a1	Tier 1	Compliance Management Asset Identification Management	4. Ownership 5. Implement'n	PO9 Assess and Manage IT Risks DS9 Manage the Configuration
Discrepancies identified in this reconciliation are promptly recorded, analyzed and the root cause is determined.	4.5.3.2.a2	Tier 1	Compliance Management Asset Identification Management	4. Ownership 5. Implement'n	DS10 Manage Problems PO4.8 Responsibility for Risk, Security and Compliance
Follow up actions are prioritized and executed.	4.5.3.2.a3	Tier 1	Program Management Asset Identification Management	4. Ownership 5. Implement'n	PO4.8 Responsibility for Risk, Security and Compliance

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
4.5.4 Software Asset Security Compliance The objective of the Software asset security compliance process is to ensure that security requirements related to the use of software and related assets are complied with.					
Implementation of the Software asset security compliance process will enable the organization to demonstrate that:	4.5.4.2				PO1 Define a Strategic IT Plan PO3 Determine Technological Direction P010 Manage projects DS5 Ensure Systems Security
Actual practice against policy is reviewed at least annually.	4.5.4.2.a	Tier 3	Policy Management	4. Ownership 7.Security: Compliance with Security Requirements	PO9 Assess and Manage IT Risks DS9 Manage the Configuration
Follow-up on any discrepancies identified in this review takes place and is documented.	4.5.4.2.b	Tier 4	Policy Management Program Management	4. Ownership 7. Security	PO4.8 Responsibility for Risk, Security and Compliance
4.5.5 Conformance Verification for SAM The objective of the Conformance verification for SAM process is to ensure that there is continuing compliance with the requirements of this part of ISO/IEC 19770 including compliance with required policies and procedures.					
Implementation of the Conformance verification for SAM process will enable the organization to demonstrate that:	4.5.5.2				PO1 Define a Strategic IT Plan PO3 Determine Technological Direction P010 Manage projects ME2 Monitor and evaluate internal control ME3 Ensure compliance with external requirements
Policies and procedures are developed, approved and issued for verifying compliance with the relevant tier(s) of this part of ISO/IEC 19770, which ensure verification at least on a sample basis annually against all of the requirements specified in the relevant tier(s) of this part of ISO/IEC 19770. This shall include verification that procedures implemented by the organization for other SAM processes are meeting all requirements specified in this part of ISO/IEC 19770 for those procedures.	4.5.5.2.a	Tier 1 - 4	Compliance Management Policy Management Communication & Education Management	1. Policy	ME2 Monitor and evaluate internal control ME3 Ensure compliance with external requirements PO1 Define a Strategic IT Plan PO2.4 Integrity Management PO4 Define the IT Processes, Organization and Relationships PO4.14 Contracted Staff Policies and Procedures
Documentary evidence exists that demonstrates (a) that the verification procedures above are being performed, and (b) that corrective follow-up action is taken until successful completion on the causes of all identified exceptions.	4.5.5.2.b	Tier 1 - 4	Compliance Management Documentation Management	1. Policy	ME2 Monitor and evaluate internal control ME3 Ensure compliance with external requirements PO4.8 Responsibility for Risk, Security and Compliance

ISO/IEC 19770-1 Key Area Outcomes	19770-1 Reference	19770-1 Tier	IAITAM Best Practice Library (IBPL) Key Area	Japanese SAMAC Best Practice	CobiT 4.1 Key Area
4.6 Operations Management Processes and Interfaces for SAM The objective of the Operations management processes and interfaces for SAM is to execute operational management functions which are essential to achieving overall SAM objectives and benefits.					
4.6.2 Relationship and contract management for SAM The objective of the Relationship and contract management for SAM process is to manage relationships with other organizations, both external and internal, to ensure the provision of seamless, quality SAM services, and to manage all contracts for software and related assets and services.					
Implementation of the Relationship and contract management for SAM process will enable the organization to demonstrate that:	4.6.2.2				PO1 Define a Strategic IT Plan PO3 Determine Technological Direction P010 Manage projects
Policies and procedures are developed, approved and issued for managing relationships with suppliers providing software and related assets and services, to include:	4.6.2.2.a	Tier 3	Vendor Management	8. Operations Management: SAM Operations Management Processes	AI5 Procure IT Resources PO1 Define a Strategic IT Plan PO2.4 Integrity Management PO4 Define the IT Processes, Organization and Relationships PO4.14 Contracted Staff Policies and Procedures
Definitions of responsibilities for supplier management with individuals assigned to have clear overall responsibility for managing each supplier.	4.6.2.2.a1	Tier 3	Vendor Management	8. Operations Management	AI5 Procure IT Resources PO2 Define the Information Architecture PO3 Determine Technological Direction PO4 Define the IT Processes, Organization and Relationships AI1 Identify Automated Solutions AI5 Procure IT Resources DS2 Manage Third-party Services
Developing invitations to tender for the supply of software or related services; to ensure that the process includes consideration of requirements for SAM, including service level management, security controls, release and change management.	4.6.2.2.a2	Tier 3	Acquisition Management Compliance Management Program Management	8.Operations Management	DS2 Manage Third-party Services
Formal documented reviews at least 6-monthly of supplier performance, achievements and issues, with documented conclusions and decisions about any actions to be taken.	4.6.2.2.a3	Tier 3	Vendor Management	8.Operations Management	DS2 Manage Third-party Services
Policies and procedures are developed, approved and issued for managing customer-side relationships, to include:	4.6.2.2.b4	Tier 4		8.Operations Management	PO1 Define a Strategic IT Plan PO2.4 Integrity Management PO4 Define the IT Processes, Organization and Relationships PO4.14 Contracted Staff Policies and Procedures
Definitions of responsibilities for managing customer-side business relationships with respect to software and related assets and services.	4.6.2.2.b5	Tier 4	Acquisition Management Vendor Management	8.Operations Management	DS1 Define and manage service levels PO8 Manage Quality
A formal review at least annually of current and future software requirements of customers and the business as a whole.	4.6.2.2.b6	Tier 4	Program Management	8.Operations Management	DS1 Define and manage service levels PO8 Manage Quality PO9 Assess and Manage IT Risks DS9 Manage the Configuration
Formal documented reviews at least annually of service provider performance, customer satisfaction, achievements and issues, with documented conclusions and decisions about any actions to be taken.	4.6.2.2.b7	Tier 4	Vendor Management Program Management	8.Operations Management	DS1 Define and manage service levels PO8 Manage Quality ME1 Monitor and evaluate IT performance PO9 Assess and Manage IT Risks DS9 Manage the Configuration