INTERNATIONAL STANDARD

ISO/IEC 19770-1

First edition
2006-05-01

Information technology — Software asset management —

Part 1: **Processes**

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

Partie 1: Procédés

Reference number
ISO/IEC 19770-1:2006(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

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*.

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

- *Part 1: Processes*
- *Part 2: Tag*

Introduction

This part of ISO/IEC 19770 has been developed to enable an organization to prove that it is performing Software Asset Management (SAM) to a standard sufficient to satisfy corporate governance requirements and ensure effective support for IT service management overall. This part of ISO/IEC 19770 is intended to align closely to, and to support, ISO/IEC 20000. Good practice in SAM should result in the following types of benefits, and certifiable good practice should allow management and other organizations to place reliance on the adequacy of these processes, and the expected benefits should be achieved with a high degree of confidence:

a) **Risk management**: SAM should facilitate the management of business risks including:

   1) risk of interruption to IT services;

   2) risk of deterioration in the quality of IT services;

   3) legal and regulatory exposure;

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

b) **Cost control**: SAM should facilitate cost control including in the following areas:

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

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

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

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

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

c) **Competitive advantage**: SAM should help the organization gain competitive advantage through the following:

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

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

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

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

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

INTERNATIONAL STANDARD **ISO/IEC 19770-1:2006(E)**

Information technology — Software asset management —

Part 1: **Processes**

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).

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 specification for SAM data, 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 an assessment framework that is aligned to the requirements in ISO/IEC15504-2.

This part of ISO/IEC 19770 applies to all organizations of any size or sector. This part of ISO/IEC 19770 can only be applied to a legal entity, or to parts of a single legal entity.

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

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. 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).

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.

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 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	Physical 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 done on this basis
	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.

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

The requirements in this part of ISO/IEC 19770 are contained in the outcomes of Clause 4. 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. It is also possible to selectively choose outcomes for individual agreements, as explained below, but conformance with this part of ISO/IEC 19770 may not then be cited.

2.2 Full conformance

Full conformance is achieved by demonstrating that all of the requirements of this part of ISO/IEC 19770 have been satisfied using the outcomes as evidence.

2.3 Agreement compliance

This part of ISO/IEC 19770 may be used to help develop an agreement between an acquirer and a supplier, in which case clauses of this part of ISO/IEC 19770 can be selected for incorporation in the agreement with or without modification. In this case, it is necessary for the acquirer and supplier to achieve compliance with the agreement rather than conformity with this part of ISO/IEC 19770.

NOTE 1 Supplier agreements usually specify the organizational scope of control, for example across all subsidiaries of a corporate entity, which means the scope of SAM will need to be set up to match this, if the intention is to move into such an agreement.

NOTE 2 ISO/IEC's copyright extends to all of this part of ISO/IEC 19770 and parts thereof. However, for the specific use mentioned in the clause above, there is no need to obtain copyright permission.

3 Terms and definitions

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

3.1
baseline
formally approved version of a configuration item (3.2), regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle (as also defined in ISO/IEC 12207)

3.2
configuration item
CI
item or aggregation of hardware or software or both that is designed to be managed as a single entity

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

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
version of the software that is used to install the software and to create distribution copies

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 An effective license consists of one or more underlying licenses (3.15).

EXAMPLE 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.

3.7
local SAM owner
individual at any level of the organization below that of the SAM owner (3.11) 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
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 (3.10).

3.10
process
a 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 (3.9).

3.11
SAM owner
individual at a senior organization-wide level who is identified as being responsible for SAM

3.12
software asset management
SAM
effective management, control and protection of software assets within an organization

3.13
software header
information about a software file to facilitate its management, embedded within the file itself

NOTE The software header is one type of information within the more generic category of software tag (3.14) information.

3.14
software tag
information about a software file or package to facilitate its management, some of which information may be held within a software header (3.13)

3.15
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).

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.

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.

4.1.2 Overview of SAM processes

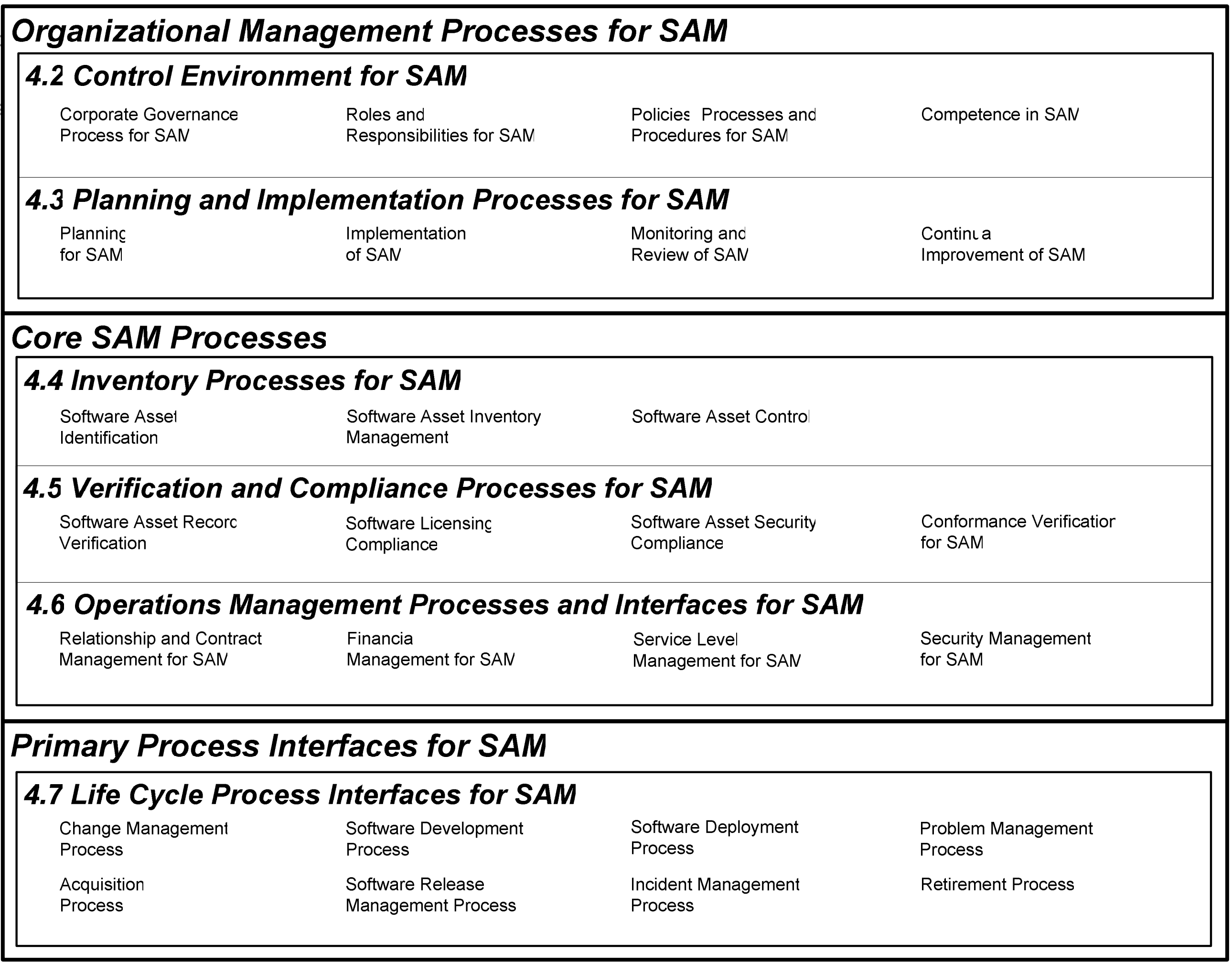
Figure 1 below gives the conceptual framework for the SAM processes and is broken down into three main categories:

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



Organizational Management Processes for SAM

4.2 Control Environment for SAM

Corporate Governance Process for SAN

Roles and Responsibilities for SAM

Policies Processes and Procedures for SAM

Competence in SAN

4.3 Planning and Implementation Processes for SAM

Planninc for SAM

Implementation of SAN

Monitoring anc Review of SAN

Continι a Improvement of SAM

Core SAM Processes

4.4 Inventory Processes for SAM

Software Asset Identification

Software Asset Inventory Management

Software Asset Contro

4.5 Verification and Compliance Processes for SAM

Software Asset Recorc Verification

Software Licensinc Compliance

Software Asset Security Compliance

Conformance Verificatior for SAM

4.6 Operations Management Processes and Interfaces for SAM

Relationship and Contract Management for SAN

Financia Management for SAN

Service Level Management for SAN

Security Management for SAM

Primary Process Interfaces for SAM

4.7 Life Cycle Process Interfaces for SAM

Change Managemenl Process

Software Development Process

Software Deployment Process

Problem Management Process

Acquisition Process

Software Release Management Process

Incident Management Process

Retirement Process

Figure 1 — 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 objective of the *Control environment for SAM* is to establish and maintain the management system within which the other SAM processes are implemented.

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

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.

4.2.2.2 Outcomes

Implementation of the *Corporate governance process for SAM* will enable the organization to demonstrate that:

a) There is a clear corporate statement 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 licensing non-compliance.

3) Risk of interruption of operations due to problems with the IT infrastructure which could result from inadequate SAM.

4) Risk of excessive spending on licensing and other IT support costs due to inadequate SAM.

5) Risks associated with decentralized vs. centralized management approaches for software and related assets.

NOTE Decentralized management 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.

6) 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 should include in particular any which link into regulatory or corporate governance requirements.

4.2.3.2 Outcomes

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 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 SAM plan.

2) Delivering results against the 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.

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.

4.2.4.2 Outcomes

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.

d) 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.

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.

4.2.5.2 Outcomes

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.

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 certifications 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 objective of *Planning and implementation processes for SAM* is to ensure the effective and efficient accomplishment of SAM management objectives.

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

Planning and implementation processes for SAM consists of the following:

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.

4.3.2.2 Outcomes

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 ('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.

   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 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.

4.3.3.2 Outcomes

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.

4.3.4.2 Outcomes

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

   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.

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.

4.3.5.2 Outcomes

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

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.

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

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.

4.4.2.2 Outcomes

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 platforms on which software can be installed or run

      ii) Software definitive master versions and distribution copies

      iii) Software builds and releases (originals and distribution copies)

      iv) All installed software

      v) Software versions

      vi) Patches and updates

      vii) Licences including underlying licenses and effective full licenses

      viii) Proof of license documentation

      ix) Contracts (including terms and conditions) relating to software assets, including both hard-copy and electronic

      x) Both physical and electronic stores of the above, as relevant

      xi) Licensing models

   3) Software should 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 Data validation requirements may also be defined as part of this process.

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.

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.

4.4.3.2 Outcomes

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 platforms 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.

   3) underlying licenses and effective full licenses held.

   NOTE There is no requirement for physically 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 sources 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.

4.4.4.2 Outcomes

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

The objective of *Verification and compliance processes for SAM* is to detect and manage all exceptions to SAM policies, processes, and procedures; including licence 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.

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

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.

4.5.2.2 Outcomes

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) At least quarterly there is reconciliation between what is installed on each platform and what was authorized for installation, including reporting on exceptions identified.

2) The hardware inventory including locations is verified at least 6-monthly, including reporting on exceptions identified.

3) The inventory of software programs (definitive master versions and distribution copies) is verified at least 6-monthly, including reporting on exceptions identified.

4) The inventory of software builds (originals and distribution copies) is verified at least 6-monthly, including reporting on exceptions identified.

5) The physical store of proof of license documentation is verified (including for authenticity) at least annually, including reporting on exceptions identified.

6) 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.

7) The physical store of contractual documentation related to software assets is verified for completeness at least annually, including reporting on exceptions identified.

8) The contracts inventory is verified at least annually, including reporting on exceptions identified.

9) Follow-up corrective actions on any discrepancies or issues identified above take place and are documented.

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.

4.5.3.2 Outcomes

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 licences owned and licences required for software used, taking into account the way licensing requirements are determined as per license terms and conditions.

NOTE This includes in particular license requirements determined on bases other than installed copies, such as server access rights.

2) Discrepancies identified in this reconciliation are promptly recorded, analysed and the root cause is determined.

3) Follow up actions are prioritised 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.

4.5.4.2 Outcomes

Implementation of the *Software asset security compliance* process will enable the organization to demonstrate that:

a) Actual practice against policy is reviewed at least annually.

NOTE This should include 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.

4.5.5.2 Outcomes

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 this part of ISO/IEC 19770, which ensure verification at least on a sample basis annually against all of the requirements specified in 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

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.

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

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

4.6.2.2 Outcomes

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.

   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.

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.

4.6.3.2 Outcomes

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.

NOTE The asset types used in financial management should be aligned with or mapped to the asset types in SAM if there are differences.

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.

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.

4.6.4.2 Outcomes

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 17799 provides guidance on information security management. Organizations certified to ISO/IEC 17799 should satisfy the security requirements within this part of ISO/IEC 19770.

4.6.5.2 Outcomes

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.

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. The objective of this part of ISO/IEC 19770 is to specify SAM requirements for these life cycle processes.

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

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.

4.7.2.2 Outcomes

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.

4.7.3.2 Outcomes

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.

   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 licence management purposes.

   2) Ensuring the receipt and safe-keeping of valid proof of license for all licences purchased.

   NOTE This may require checking for authenticity of proof of licence, 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.

4.7.4.2 Outcomes

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) Licence constraints and dependencies.

b) There is a formal process for software development ensuring that software products are placed under software asset control.

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* works together closely with the *Change management process*.

4.7.5.2 Outcomes

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 in some way before distribution.

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.

4.7.6.2 Outcomes

Implementation of the *Software deployment process* will enable the organization to demonstrate that:

a) Policies and procedures are developed, approved and issued for distributing and installing software to include the following:

1) The distribution 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 distributed and after it is installed.

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.

5) There is a documented control to verify that what was deployed is the same as what was authorized to be deployed.

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.

4.7.7.2 Outcomes

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.

4.7.8.2 Outcomes

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.

4.7.9.2 Outcomes

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.

   2) Licenses and other assets which can be redeployed are identified for redeployment.

   3) Any assets transferred to other parties (whether those parties are 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.

ISO/IEC 19770-1:2006(E)

ICS 35.080

Price based on 25 pages