INTERNATIONAL STANDARD

ISO/IEC 19770-1

Third edition
2017-12

Information technology — IT asset management —

Part 1: IT asset management systems — Requirements

Technologies de l'information — Gestion des actifs logiciels — Partie 1: Procédés et évaluation progressive de la conformité

Reference number
ISO/IEC 19770-1:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and system engineering*. Participation and contributions were requested in particular from ISO/IEC JTC 1/SC 27 *IT Security Techniques*, ISO/IEC JTC 1/SC 40 *IT Service Management and IT Governance*, and ISO/TC 251 *Asset Management*.

This third edition cancels and replaces the second edition (ISO/IEC 19770-1:2012), which has been technically revised to be a Management System Standard.

A list of all parts in the ISO/IEC 19770 series can be found on the ISO website.

Introduction

This document specifies the requirements for the establishment, implementation, maintenance and improvement of a management system for IT asset management (ITAM), referred to as an “IT asset management system” (ITAMS).

This document provides additional requirements to ISO 55001:2014 which specifies the requirements for the establishment, implementation, maintenance and improvement of a management system for asset management, referred to as an “asset management system”. This document includes additional or more detailed requirements which are considered necessary for the management of IT assets. The primary differentiator is the need to manage software assets, with their specific characteristics. Although ISO 55001:2014 can be used to manage software assets if organizations define their scope and relevant requirements appropriately, it is primarily focused on physical assets with little provision for the management of software assets.

There are a number of characteristics of IT assets which create these additional or more detailed requirements. These are described in Annex C. As a result of these characteristics of IT assets, a management system for IT assets will consequently have explicit requirements additional to those in ISO 55001:2014 dealing with:

— controls over software modification, duplication and distribution, with particular emphasis on access and integrity controls;

— audit trails of authorizations and of changes made to IT assets;

— controls over licensing, underlicensing, overlicensing, and compliance with licensing terms and conditions;

— controls over situations involving mixed ownership and responsibilities, such as in cloud computing and with ‘Bring-Your-Own-Device’ (BYOD) practices; and

— reconciliation of IT asset management data with data in other information systems when justified by business value, in particular with financial information systems recording assets and expenses.

Furthermore, because information associated with IT assets is typically voluminous, highly complex and fast-changing, it is likely that organizations with such information will need to make use of automated information systems.

Another difference between ISO 55001:2014 and this document is that this document provides optionally for multiple explicit groupings of process objectives (or 'tiers'). The most important of these is the basic tier called 'trustworthy data', which is the most important to most end-user organizations and also software publishers. Tier two is for ‘life cycle integration’, and tier three is for ‘optimization’. More information about the tiers and their respective groupings of objectives is given in Annex B.

Since major physical assets increasingly incorporate or depend on software, it is likely that the additional requirements of this document will be relevant in such situations. It is likely that most organizations with major physical assets will need management systems meeting a mixture of 'pure' ISO 55001:2014 requirements and also of the additional requirements from this document.

IT assets encompass a wide variety of asset types. Figure 1 indicates the principal IT asset types diagrammatically.

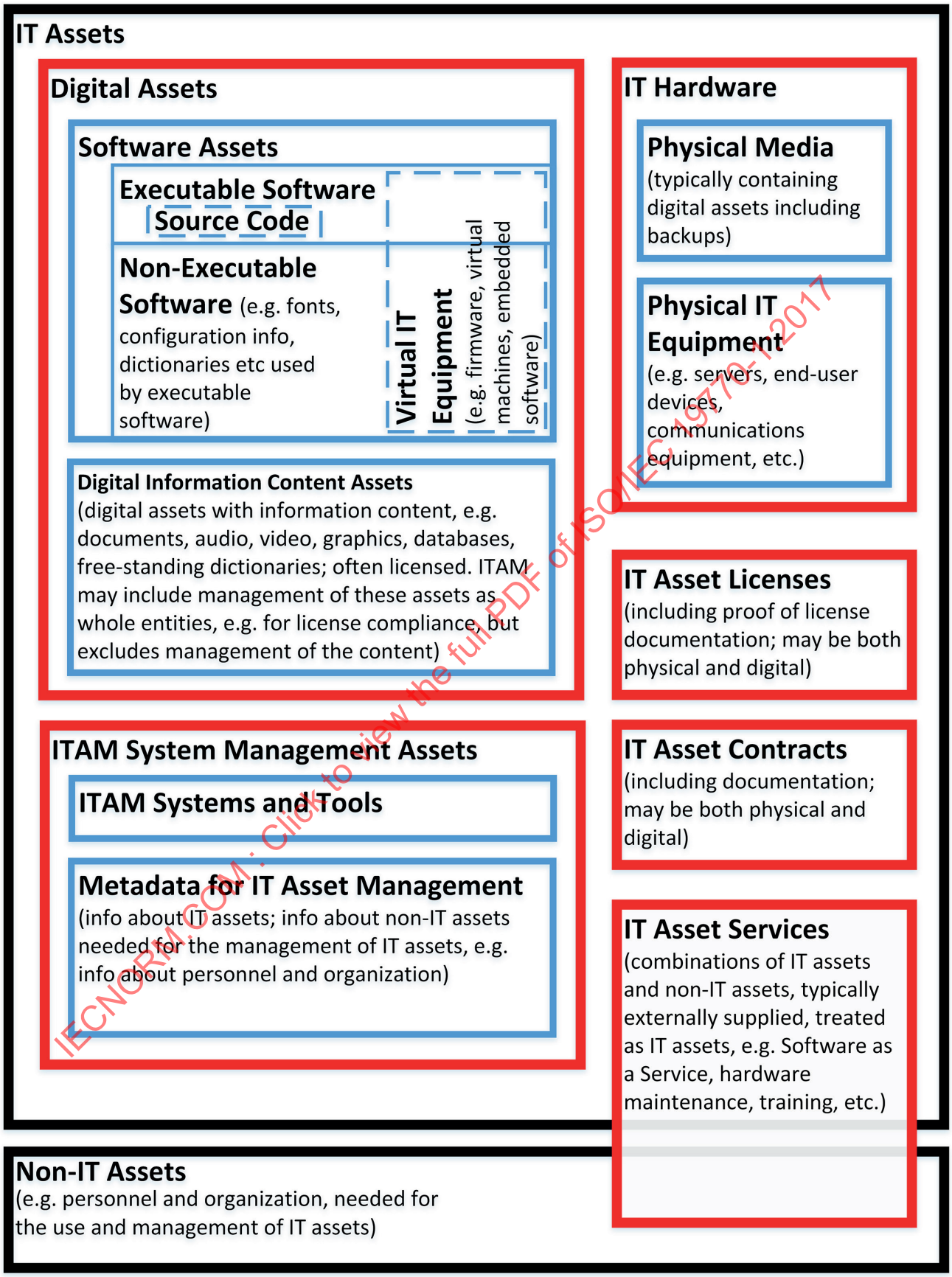

Figure 1 — Principal types of IT assets

This document can be used by any organization and can be applied to all types of IT assets. The organization determines to which of its IT assets this document applies.

This document is primarily intended for use by:

— those involved in the establishment, implementation, maintenance, and improvement of an IT asset management system;

— those involved in delivering IT asset management activities, including service providers;

— internal and external parties to assess the organization's ability to meet legal, regulatory and contractual requirements and the organization's own requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented.

Further guidance regarding the application of the requirements within this document shared with ISO 55001:2014 is provided in ISO 55002.

General information on asset management and on IT asset management, and information on the terminology applicable to this document, is provided in ISO 55000 and in ISO/IEC 19770-5. Organizations can find that these documents will assist in the development of IT asset management in their organization.

This document applies the definition of "risk" given in ISO 31000:2009 and ISO/IEC Guide 73:2009. In addition, it uses the term "stakeholder" rather than "interested party".

This document is designed to enable an organization to align and integrate its IT asset management system with related management system requirements, for example those specified by ISO/IEC 27001 and ISO/IEC 20000-1.

This document is not intended to be in conflict with any organization's policies, procedures and standards. Any such conflict should be resolved before using this document.

Information technology — IT asset management —

Part 1:
IT asset management systems — Requirements

1 Scope

1.1 Purpose

This document specifies requirements for an IT asset management system within the context of the organization.

This document can be applied to all types of IT assets and by all types and sizes of organizations.

NOTE 1 This document is intended to be used for managing IT assets in particular, but it can also be applied to other asset types. It can be suitable, in whole or in part, for managing embedded software and firmware, however its use for these purposes has not been determined. It is not intended for managing information assets per se, i.e. it is not intended for managing information as an asset independent of hardware and software assets. Certain types of data and information are covered, such as data and information about IT assets in scope, and depending on how the scope is defined, it can cover digital information content assets. See the Introduction for an explanation about IT assets.

NOTE 2 This document does not specify financial, accounting, or technical requirements for managing specific IT asset types.

NOTE 3 For the purposes of this document, the term "IT asset management system" is used to refer to a management system for IT asset management.

This document is a discipline-specific extension of ISO 55001:2014, with changes, and is not a sector-specific application of that International Standard. ISO 55001:2014 is intended to be used for managing physical assets in particular, but it can also be applied to other asset types. This document specifies requirements for the management of IT assets which are additional to those specified in ISO 55001:2014. Conformance to this document does not imply conformance to ISO 55001:2014.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own IT asset management requirements.

1.2 Field of application

This document applies to IT asset management processes and can be implemented by organizations to achieve immediate benefits.

This document can be applied to all IT assets. For example, it can be applied to not only IT hardware but also to executable software (such as application programs and operating systems) and non-executable software (such as fonts and configuration information). 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 legacy computing environments).

1.3 Limitations

This document does not detail the IT asset management processes in terms of methods or procedures required to meet the requirements for outcomes of a process.

This document does not specify the sequence of steps an organization should follow to implement IT asset management.

This document does not detail documentation in terms of name, format, explicit content and recording media.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

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

Some of these terms are repeated from ISO 55000:2014, and refer to assets in general. These terms are usable for IT assets when used in the context of IT asset management, with 'asset' being understood as referring to 'IT asset'. In some cases, terms specific to IT assets have been added. No specific interpretation is intended based on whether an IT-specific term has been defined or not.

3.1
asset
item, thing or entity that has potential or actual value to an *organization* (3.38)

Note 1 to entry: Value can be tangible or intangible, financial or non-financial, and includes consideration of *risks* (3.48) and liabilities. It can be positive or negative at different stages of the *asset life* (3.2).

Note 2 to entry: Physical assets usually refer to equipment, inventory and properties owned by the organization. Physical assets are the opposite of intangible assets, which are non-physical assets such as leases, brands, digital assets, use rights, licences, intellectual property rights, reputation or agreements.

Note 3 to entry: A grouping of assets referred to as an *asset system* (3.7) could also be considered as an asset.

[SOURCE: ISO 55000:2014, 3.2.1]

3.2
asset life
period from *asset* (3.1) creation to asset end-of-life

[SOURCE: ISO 55000:2014, 3.2.2]

3.3
asset management
coordinated activity of an *organization* (3.38) to realize value from *assets* (3.1)

Note 1 to entry: Realization of value will normally involve a balancing of costs, *risks* (3.48), opportunities and *performance* (3.42) benefits.

Note 2 to entry: Activity can also refer to the application of the elements of the *asset management system* (3.5).

Note 3 to entry: The term "activity" has a broad meaning and can include, for example, the approach, the planning, the plans and their implementation.

[SOURCE: ISO 55000:2014, 3.3.1]

3.4
asset management plan
documented information (3.19) that specifies the activities, resources and timescales required for an individual *asset* (3.1), or a grouping of assets, to achieve the *organization's* (3.38) *asset management* (3.3) *objectives* (3.37)

Note 1 to entry: The grouping of assets may be by *asset type* (3.8), asset class, *asset system* (3.7) or *asset portfolio* (3.6).

Note 2 to entry: An asset management plan is derived from the *strategic asset management plan* (3.53).

Note 3 to entry: An asset management plan may be contained in, or may be a subsidiary plan of, the strategic asset management plan.

[SOURCE: ISO 55000:2014, 3.3.3]

3.5
asset management system
management system (3.33) for *asset management* (3.3) whose function is to establish the asset management *policy* (3.43) and asset management *objectives* (3.37)

Note 1 to entry: The asset management system is a subset of asset management.

[SOURCE: ISO 55000:2014, 3.4.3]

3.6
asset portfolio
assets (3.1) that are within the scope of the *asset management system* (3.5)

Note 1 to entry: A portfolio is typically established and assigned for managerial control purposes. Portfolios for physical hardware might be defined by category (e.g. plant, equipment, tools, land). Software portfolios might be defined by software publisher, or by platform (e.g. PC, server, mainframe).

Note 2 to entry: An asset management system can encompass multiple asset portfolios. Where multiple asset portfolios and asset management systems are employed, *asset management* (3.3) activities should be coordinated between the portfolios and systems.

[SOURCE: ISO 55000:2014, 3.2.4]

3.7
asset system
set of *assets* (3.1) that interact or are interrelated

[SOURCE: ISO 55000:2014, 3.2.5]

3.8
asset type
grouping of *assets* (3.1) having common characteristics that distinguish those assets as a group or class

EXAMPLE Physical assets, information assets, intangible assets, *critical assets* (3.15), enabling assets, linear assets, information and communications technology (ICT) assets, infrastructure assets, moveable assets.

[SOURCE: ISO 55000:2014, 3.2.6]

3.9
audit
systematic, independent and documented *process* (3.46) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined or integrated audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the organization itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

[SOURCE: ISO 55000:2014, 3.1.1, modified — Note 2 to entry has been added for conformance with Annex SL]

3.10
capability
<asset management> measure of capacity and the ability of an entity (system, person or *organization* (3.38)) to achieve its *objectives* (3.37)

Note 1 to entry: *Asset management* (3.3) capabilities include *processes* (3.46), resources, *competences* (3.11) and technologies to enable the effective and efficient development and delivery of *asset management plans* (3.4) and *asset life* (3.2) activities, and their *continual improvement* (3.13).

[SOURCE: ISO 55000:2014, 3.1.2]

3.11
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO 55000:2014, 3.1.3]

3.12
conformity
fulfilment of a *requirement* (3.47)

[SOURCE: ISO 55000:2014, 3.1.4]

3.13
continual improvement
recurring activity to enhance *performance* (3.42)

[SOURCE: ISO 55000:2014, 3.1.5]

3.14
corrective action
action to eliminate the cause of a *nonconformity* (3.36) and to prevent recurrence

Note 1 to entry: In the case of other undesirable outcomes, action is necessary to minimize or eliminate the causes and to reduce the impact or prevent recurrence. Such actions fall outside the concept of corrective action, in the sense of this definition.

[SOURCE: ISO 55000:2014, 3.4.1]

3.15
critical asset
asset (3.1) having potential to significantly impact on the achievement of the *organization's* (3.38) *objectives* (3.37)

Note 1 to entry: Assets can be safety-critical, environment-critical or *performance-critical* (3.42) and can relate to legal, regulatory or statutory *requirements* (3.47).

Note 2 to entry: Critical assets can refer to those assets necessary to provide services to critical customers.

Note 3 to entry: *Asset systems* (3.7) can be distinguished as being critical in a similar manner to individual assets.

[SOURCE: ISO 55000:2014, 3.2.7]

3.16
data
facts about an object

Note 1 to entry: In the context of *IT asset management systems* (3.28), data may be a captured, measured or recorded representation of information, before it is analysed, interpreted or processed. Data may relate to objects such as facts, events, things, processes, or ideas, including concepts that within a certain context have a particular meaning related to IT assets.

[SOURCE: ISO 9000:2015, 3.8.1, modified — Note 1 has been added, modified from ISO 15784-1 and ISO/IEC 2382]

3.17
digital asset
IT asset (3.25) expressed electronically in a digital format

Note 1 to entry: Digital assets include *software assets* (3.50), and *digital information content assets* (3.18).

3.18
digital information content asset
digital asset (3.17) with information content

EXAMPLE Documents, audio, video, graphics, databases, free-standing dictionaries; often licensed.

Note 1 to entry: ITAM can include management of these assets as whole entities, e.g. for license compliance, but excludes management of the content.

3.19
documented information
information required to be controlled and maintained by an *organization* (3.38) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.33), including related *processes* (3.46);

— information created in order for the organization to operate (documentation);

— evidence of results achieved (e.g. records, key performance indicators).

[SOURCE: ISO 55000:2014, 3.1.6]

3.20
effectiveness
extent to which planned activities are realized and planned results achieved

[SOURCE: ISO 55000:2014, 3.1.7]

3.21
hardware
physical equipment used to process, store, or transmit computer programs or data

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.1278]

3.22
incident
unplanned event or occurrence resulting in damage or other loss

[SOURCE: ISO 55000:2014, 3.1.8]

3.23
information
meaningful data

Note 1 to entry: In the context of *IT asset management systems* (3.28), information may be data that has been converted, analysed, interpreted or compiled, to which meaning is assigned, according to context and assumed conventions. The underlying data may relate to objects such as facts, events, things, processes, or ideas, including concepts, that within a certain context have a particular meaning related to *IT assets* (3.25).

Note 2 to entry: In the context of IT asset management systems, information may be recorded digitally or physically (e.g. on paper).

[SOURCE: ISO 9000:2015, 3.8.2, modified — Note 1 to entry modified from ISO/TR 12037, ISO/TR 21089 and ISO/IEC 2382) and Note 2 to entry has been added.]

3.24
information technology
IT
development, maintenance, and use of technology to acquire, process, store and distribute digital information

Note 1 to entry: This excludes the use of technology to acquire, process, store and distribute information which is not digital, such as paper-based information. Examples which are excluded when not digitally captured are books, manuals, manuscripts, and whiteboards. For the purposes of this definition, 'digital' is equivalent to 'electronic'.

3.25
IT asset
item, thing, or entity that can be used to acquire, process, store and distribute digital information and has potential or actual value to an organization.

Note 1 to entry: IT assets include:

— *software* (3.49);

— media (physical and digital);

— IT equipment (physical and virtual);

— licenses (including proof of license);

— contracts; and

— ITAM system management assets (including ITAM systems and tools, and the metadata needed to manage all IT assets).

Note 2 to entry: Services to meet *IT asset management* (3.26) *requirements* (3.47), typically externally supplied, can also be considered IT assets, such as 'software-as-a-service', hardware maintenance, software support, and training.

Note 3 to entry: *Digital information content assets* (3.18) are files or other entities with information content, but they are not considered software. For example, there may be collections of standards in digital form; media collections; and credit agency rating information. Such assets may be licensed, and therefore may benefit from being managed using the discipline of IT asset management.

Note 4 to entry: Information per se, independent of IT hardware and software assets, can be considered an *asset* (3.1), but it is not considered an IT asset.

Note 5 to entry: The collective set of IT assets is also referred to as the *IT infrastructure* (3.30).

3.26
IT asset management
ITAM
coordinated activity of an *organization* (3.38) to realize value from *IT assets* (3.25)

3.27
IT asset management plan
documented information (3.19) that specifies the activities, resources and timescales required for an individual *IT asset* (3.25), or a grouping of IT assets, to achieve the *organization's* (3.38) *IT asset management* (3.26) *objectives* (3.37)

Note 1 to entry: The grouping of assets may be by *asset type* (3.8), asset class, *asset system* (3.7) or *IT asset portfolio* (3.29).

Note 2 to entry: An IT asset management plan is derived from the *strategic IT asset management plan* (3.54).

Note 3 to entry: An IT asset management plan may be contained in, or may be a subsidiary plan of, the strategic IT asset management plan.

[SOURCE: ISO 55000:2014, 3.3.3, modified — asset management plan has become IT asset management plan and all notes have been made discipline-specific]

3.28
IT asset management system
ITAMS
management system (3.33) for *IT asset management* (3.26) whose function is to establish the IT asset management *policy* (3.43) and IT asset management *objectives* (3.37)

Note 1 to entry: The asset management system is a subset of asset management.

[SOURCE: ISO 55000:2014, 3.4.3, modified — asset management system has become IT asset management system and definition as well as notes have become discipline-specific]

3.29
IT asset portfolio
IT assets (3.25) that are within the scope of the *IT asset management system* (3.28)

Note 1 to entry: A portfolio is typically established and assigned for managerial control purposes. Portfolios for IT hardware might be defined by category (e.g. servers, PCs, mobile devices). Software portfolios might be defined by software publisher, or by platform (e.g. PC, server, mainframe).

Note 2 to entry: An IT asset management system can encompass multiple IT asset portfolios.

Note 3 to entry: See also *asset portfolio* (3.6).

3.30
IT infrastructure
combined set of *IT assets* (3.25) for developing, maintaining, and using IT services

3.31
level of service
parameters, or combination of parameters, which reflect social, political, environmental and economic outcomes that the *organization* (3.38) delivers

Note 1 to entry: The parameters can include safety, customer satisfaction, quality, quantity, capacity, reliability, responsiveness, environmental acceptability, cost and availability.

[SOURCE: ISO 55000:2014, 3.3.6]

3.32
life cycle
stages involved in the management of an *asset* (3.1)

Note 1 to entry: The naming and number of the stages and the activities under each stage usually vary in different industry sectors and are determined by the *organization* (3.38).

[SOURCE: ISO 55000:2014, 3.2.3]

3.33
management system
set of interrelated or interacting elements of an *organization* (3.38) to establish *policies* (3.43) and *objectives* (3.37) and *processes* (3.46) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning, and operation, etc.

Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

[SOURCE: ISO 55000:2014, 3.4.2, modified — 'and' has been added to Note 2 to entry for conformance with Annex SL]

3.34
measurement
process (3.46) to determine a value

[SOURCE: ISO 55000:2014, 3.1.10]

3.35
monitoring
determining the status of a system, a *process* (3.46) or an activity

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

Note 2 to entry: For the purposes of asset management, monitoring may also refer to determining the status of an asset. This is typically referred to as "condition monitoring" or "performance monitoring".

[SOURCE: ISO 55000:2014, 3.1.9]

3.36
nonconformity
non-fulfilment of a *requirement* (3.47)

Note 1 to entry: Nonconformity can be any deviation from *asset management system* (3.5) requirements, or from relevant work standards, practices, procedures, legal requirements, etc.

[SOURCE: ISO 55000:2014, 3.1.11]

3.37
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and *process* (3.46)).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an *asset management* (3.3) objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of *asset management systems* (3.5), asset management objectives are set by the *organization* (3.38), consistent with the *organizational objectives* (3.39) and *asset management policy* (3.43), to achieve specific measurable results.

[SOURCE: ISO 55000:2014, 3.1.12, modified — 'as' has been added to Note 3 for conformance with Annex SL]

3.38
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.37)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO 55000:2014, 3.1.13]

3.39
organizational objective
overarching *objective* (3.37) that sets the context and direction for an *organization's* (3.38) activities

Note 1 to entry: Organizational objectives are established through the strategic level planning activities of the organization.

[SOURCE: ISO 55000:2014, 3.1.14]

3.40
organizational plan
documented information (3.19) that specifies the programmes to achieve the *organizational objectives* (3.39)

[SOURCE: ISO 55000:2014, 3.1.15]

3.41
outsource (verb)
make an arrangement where an *external organization* (3.38) performs part of an organization's function or *process* (3.46)

Note 1 to entry: An external organization is outside the scope of the *management system* (3.33), although the outsourced function or process is within the scope if its activities influence the effectiveness of the *asset management system* (3.5).

[SOURCE: ISO 55000:2014, 3.1.16]

3.42
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.46), products (including services), systems or *organizations* (3.38).

Note 3 to entry: For the purposes of *asset management* (3.3), performance can relate to *assets* (3.1) in their ability to fulfil *requirements* (3.47) or *objectives* (3.37).

[SOURCE: ISO 55000:2014, 3.1.17, modified — the spelling of 'measurable' has been changed for conformance with Annex SL]

3.43
policy
intentions and direction of an *organization* (3.38), as formally expressed by its *top management* (3.55)

[SOURCE: ISO 55000:2014, 3.1.18, modified — a comma has been added for conformance with Annex SL]

3.44
predictive action
action to monitor the condition of an *asset* (3.1) and predict the need for *preventive action* (3.45) or *corrective action* (3.14)

Note 1 to entry: Predictive action is also commonly referred to as either "condition monitoring" or "performance monitoring".

[SOURCE: ISO 55000:2014, 3.3.5]

3.45
preventive action
action to eliminate the cause of a potential *nonconformity* (3.36) or other undesirable potential situation

Note 1 to entry: This definition is specific to *asset management* (3.3) activities only.

Note 2 to entry: There can be more than one cause for a potential nonconformity.

Note 3 to entry: Preventive action is taken to prevent occurrence and to preserve an *asset's* (3.1) function, whereas *corrective action* (3.14) is taken to prevent recurrence.

Note 4 to entry: Preventive action is normally carried out while the asset is functionally available and operable or prior to the initiation of functional failure.

Note 5 to entry: Preventive action includes the replenishment of consumables where the consumption is a functional *requirement* (3.47).

[SOURCE: ISO 55000:2014, 3.3.4]

3.46
process
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: ISO 55000:2014, 3.1.19]

3.47
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.38) and *stakeholders* (3.52) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in *documented information* (3.19).

[SOURCE: ISO 55000:2014, 3.1.20]

3.48
risk
effect of uncertainty on *objectives* (3.37)

Note 1 to entry: An effect is a deviation from the expected — positive and/or negative.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and *process* (3.46)).

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

[SOURCE: ISO 55000:2014, 3.1.21, modified — wording has been added to Note 4 for conformance with Annex SL]

3.49
software
all or part of the programs which process or support the processing of digital information

Note 1 to entry: For the purposes of this definition, software excludes information per se, such as the content of documents, audio and video recordings, graphics, and databases.

Note 2 to entry: There is both executable and non-executable software. The purpose of non-executable software is to control or support executable software, and includes, for example, configuration information, fonts, and spell-checker dictionaries. Digital information which is managed by executable software (e.g. the content of documents and databases) is not considered software for the purposes of this definition, even though program execution may depend on data values.

3.50
software asset
software (3.49) that has potential or actual value to an organization.

Note 1 to entry: Software may be a collection of software components, e.g. a software product may be a collection of thousands of software files.

3.51
software asset management
SAM
coordinated activity of an organization to realize value from *software assets* (3.50)

Note 1 to entry: Software asset management is a specialization of *IT asset management* (3.26) focused specifically on software assets. The management of software assets may, but does not necessarily, involve the management of non-software assets.

Note 2 to entry: For reference, a corresponding industry definition is "all of the infrastructure and processes necessary for the effective management, control and protection of the software assets within an organization, throughout all stages of their life cycle"

3.52
stakeholder
person or *organization* (3.38) that can affect, be affected by, or perceive itself to be affected by a decision or activity

Note 1 to entry: A "stakeholder" can also be referred to as an "interested party".

[SOURCE: ISO 55000:2014, 3.1.22, modified — 'themselves' has been changed to 'itself' for conformance with Annex SL]

3.53
strategic asset management plan
SAMP
documented information (3.19) that specifies how *organizational objectives* (3.39) are to be converted into *asset management* (3.3) *objectives* (3.37), the approach for developing *asset management plans* (3.4), and the role of the *asset management system* (3.5) in supporting achievement of the asset management objectives

Note 1 to entry: A strategic asset management plan is derived from the *organizational plan* (3.40).

Note 2 to entry: A strategic asset management plan may be contained in, or may be a subsidiary plan of, the organizational plan.

[SOURCE: ISO 55000:2014, 3.3.2]

3.54
strategic IT asset management plan
documented information (3.19) that specifies how *organizational objectives* (3.39) are to be converted into *IT asset management* (3.26) *objectives* (3.37), the approach for developing *IT asset management plans* (3.27), and the role of the *IT asset management system* (3.28) in supporting achievement of the IT asset management objectives

Note 1 to entry: A strategic IT asset management plan is derived from the *organizational plan* (3.40).

Note 2 to entry: A strategic IT asset management plan may be contained in, or may be a subsidiary plan of, the organizational plan.

[SOURCE: ISO 55000:2014, 3.3.2, modified — term and definition have become discipline-specific]

3.55
top management
person or group of people who directs and controls an *organization* (3.38) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.33) covers only part of an organization, then top management refers to those who direct and control that part of the organization. If multiple *asset management systems* (3.5) are employed, the systems should be designed to coordinate efforts.

[SOURCE: ISO 55000:2014, 3.1.23]

3.56
trustworthy data
data (3.16) and related *information* (3.23) that is accurate, complete, relevant, readily understood by and available to those authorised users who need it to complete a task

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its IT asset management system.

NOTE Determining these issues refers to establishing the context of the organization considered in ISO 31000:2009, 5.3.

IT asset management objectives, included in the strategic IT asset management plan, shall be aligned to, and consistent with the organizational objectives.

4.2 Understanding the needs and expectations of stakeholders

The organization shall determine:

— the stakeholders that are relevant to the IT asset management system;

NOTE 1 Stakeholders include those responsible for related systems and processes, such as for Information Security Management and Service Management.

NOTE 2 Stakeholders include licensors of software where licensed software is within the scope of the IT asset management system.

— the relevant requirements and expectations of these stakeholders with respect to IT asset management;

NOTE 3 Requirements of software licensors include their licensing terms and conditions.

— the criteria for IT asset management decision making;

— the stakeholder requirements for recording financial and non-financial information relevant to IT asset management, and for reporting on it both internally and externally.

4.3 Determining the scope of the IT asset management system

The organization shall determine the boundaries and applicability of the IT asset management system to establish its scope. The scope shall be aligned with the strategic IT asset management plan and the IT asset management policy. When determining this scope, the organization shall consider:

— the external and internal issues referred to in 4.1;

— the requirements referred to in 4.2;

— the interaction with other management systems, if used.

The organization shall define the IT asset portfolio or portfolios covered by the scope of the IT asset management system.

The requirements of this document should be applied in their entirety to the IT assets determined by the organization.

The scope shall be available as documented information.

NOTE Scope defines which IT assets are covered by the IT asset management system. There is a separate consideration about which process areas are included in the IT asset management system. This consideration is addressed in 6.2.1.

4.4 IT asset management system

The organization shall establish, implement, maintain and continually improve an IT asset management system, including the processes needed and their interactions, in accordance with the requirements of this document.

The organization shall develop a strategic IT asset management plan which includes documentation of the role of the IT asset management system in supporting achievement of the IT asset management objectives.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the IT asset management system by:

— ensuring that the IT asset management policy, the strategic IT asset management plan and IT asset management objectives are established and are compatible with the strategic direction of the organization and organizational objectives;

— ensuring the integration of the IT asset management system requirements into the organization's business processes;

— ensuring that the resources needed for the IT asset management system are available;

— communicating the importance of effective IT asset management and of conforming to the IT asset management system requirements;

— ensuring that the IT asset management system achieves its intended outcome(s);

— directing and supporting persons to contribute to the effectiveness of the IT asset management system;

— promoting cross-functional collaboration within the organization;

— promoting continual improvement;

— supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility; and

— ensuring that the approach used for managing risk in IT asset management is aligned with the organization's approach for managing risk.

NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Policy

Top management shall establish an IT asset management policy that:

a) is appropriate to the purpose of the organization;

b) provides a framework for setting IT asset management objectives;

c) includes a commitment to satisfy applicable requirements; and

d) includes a commitment to continual improvement of the IT asset management system.

The IT asset management policy shall:

— be consistent with the organizational plan;

— be consistent with other relevant organizational policies, including of any other management systems used by the organization;

— be consistent with the relevant strategic plans of any other management systems used by the organization;

— be appropriate to the nature and scale of the organization's IT assets and operations;

— be appropriate to the responsibility of individual and organization concerning control of IT assets;

— be appropriate to the acceptable use of the IT assets of the organization;

— include the organization's policy towards compliance with IT asset contract terms and conditions, including software licensing;

— be available as documented information;

— be communicated within the organization;

— be available to stakeholders, as appropriate;

— include specification of the penalties for violating this policy; and

— be implemented and be periodically reviewed and, if required, updated.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) establishing and updating the strategic IT asset management plan, including IT asset management objectives;

b) ensuring that the IT asset management system supports delivery of the strategic IT asset management plan;

c) ensuring that the IT asset management system conforms to the requirements of this document;

d) ensuring the suitability, adequacy and effectiveness of the IT asset management system;

e) establishing and updating the IT asset management plan(s) (see 6.2.4); and

f) reporting on the performance of the IT asset management system to top management.

6 Planning

6.1 Actions to address risks and opportunities for the IT asset management system

6.1.1 General

When planning for the IT asset management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

— give assurance that the IT asset management system can achieve its intended outcome(s);

— prevent, or reduce undesired effects; and

— achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities, taking into account how these risks and opportunities can change with time;

b) how to:

— integrate and implement the actions into its IT asset management system processes; and

— evaluate the effectiveness of these actions.

6.1.2 IT asset risk assessment

The organization shall define and apply an IT asset risk assessment process that:

a) establishes and maintains IT asset risk criteria that include:

1) the risk acceptance criteria; and

2) criteria for performing IT asset risk assessments;

b) ensures that repeated IT asset risk assessments produce consistent, valid and comparable results;

c) identifies the IT asset risks:

1) apply the IT asset risk assessment process to identify all relevant risks, including:

a. risks associated with the loss of confidentiality, integrity and availability for IT assets within the scope of the IT asset management system;

b. business continuity risks;

c. legal and regulatory compliance risks;

d. risks associated with contractual compliance, including license compliance risk; and

2) identify the risk owners;

NOTE Risks associated with the information contained within IT assets can be assessed against the risk assessment requirements of ISO/IEC 27001. Guidance for conducting information security risk assessments can be obtained from ISO/IEC 27005.

d) analyses the IT asset risks:

1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;

2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

3) determine the levels of risk;

e) evaluates the IT asset risks:

1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the IT asset risk assessment process.

6.1.3 IT asset risk treatment

The organization shall define and apply an IT asset risk treatment process to:

a) select appropriate IT asset risk mitigation measures, taking account of the risk assessment results;

NOTE Organizations can design mitigation measures as required, or identify them from any source.

b) determine all controls that are necessary to implement the IT asset risk treatment option(s) chosen;

NOTE Organizations can design controls as required, or identify them from any source.

c) formulate an IT asset risk treatment plan; and

d) obtain IT asset owners' approval of the IT asset risk treatment plan and acceptance of the residual IT asset risks.

The organization shall retain documented information about the IT asset risk treatment process.

NOTE The risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000, and the requirements specified in ISO/IEC 27001:2013, 6.1.2 and 6.1.3.

6.2 IT asset management objectives and planning to achieve them

6.2.1 IT asset management operation process specification

The organization shall determine the operation processes which are appropriate for the degree of management assurance required with respect to IT asset management.

NOTE 1 Annex A provides a list of operation processes for IT asset management. This list is not exhaustive, and additional operation processes can be needed.

NOTE 2 It is possible but not required to specify groupings of processes for inclusion or exclusion based on their tier classification as described in Annex B.

6.2.2 IT asset management objectives for operation processes

The organization shall determine the objectives which are appropriate for the operation processes identified in 6.2.1. The objectives determined in this way shall be compared with those in Annex A.

A Statement of Applicability shall be produced which lists the objectives specified, with justification for inclusion and exclusion of any listed in Annex A.

NOTE 1 The processes and process objectives listed in Annex A are not exhaustive and additional operation processes and process objectives can be needed.

NOTE 2 The term 'Statement of Applicability' has been chosen because of its analogy with the Statement of Applicability in ISO/IEC 27001:2013. The Statement of Applicability together with the scope definition (4.3) are needed by any internal or external party to understand what is covered by the IT asset management system.

NOTE 3 It is possible but not required to specify groupings of processes and process objectives for inclusion or exclusion based on their tier classification as described in Annex B.

6.2.3 Overall IT asset management objectives

The organization shall establish IT asset management objectives at relevant functions and levels.

When establishing its IT asset management objectives, the organization shall consider the requirements of relevant stakeholders and of other financial, technical, legal, regulatory and organizational requirements in the IT asset management planning process.

NOTE 1 The overall set of IT asset management objectives builds on the IT asset management objectives for operation processes identified in 6.2.2.

The IT asset management objectives shall:

— be consistent and aligned with the organizational objectives;

NOTE 2 Organizational objectives can include objectives relating to energy efficiency and other concerns of environmental sustainability.

— be consistent with the IT asset management policy;

— be established and updated using IT asset management decision-making criteria (see 4.2);

— be established and updated as part of the strategic IT asset management plan;

— be measurable (if practicable);

— include quantitative targets for data accuracy;

— take into account applicable requirements;

— reflect (where appropriate) the likelihood of high rates of change in technology and in the business environment;

— be monitored;

— be communicated to relevant stakeholders; and

— be reviewed and updated as appropriate.

The organization shall retain documented information on the IT asset management objectives.

6.2.4 Planning to achieve IT asset management objectives

The organization shall integrate the planning to achieve IT asset management objectives with other organizational planning activities, including financial, human resources and other support functions.

The organization shall establish, document and maintain IT asset management plan(s) to achieve the IT asset management objectives. These IT asset management plan(s) shall be aligned with the IT asset management policy and the strategic IT asset management plan.

The organization shall ensure that the IT asset management plan(s) take(s) into account relevant requirements coming from outside the IT asset management system.

When planning how to achieve its IT asset management objectives, the organization shall determine and document:

a) the method and criteria for decision making and prioritizing of the activities and resources to achieve its IT asset management plan(s) and IT asset management objectives;

b) the processes and methods to be employed in managing its IT assets over their life cycles;

c) what will be done;

d) what resources will be required;

e) who will be responsible;

f) when it will be completed;

g) how the results will be evaluated;

h) the appropriate time horizon(s) for the IT asset management plan(s);

i) the financial and non-financial implications of the IT asset management plan(s);

j) the review period for the IT asset management plan(s) (see 9.1);

k) actions to address opportunities associated with managing the IT assets, taking into account how these opportunities can change with time, by establishing processes for:

   — identification of opportunities;

   — assessment of opportunities;

   — determining the significance of IT assets in achieving IT asset management objectives;

   — implementation of the appropriate treatment, and monitoring, of opportunities.

NOTE ISO 55001:2014 includes risks in this text, whereas this document addresses risks more extensively in 6.1.2 and 6.1.3 similar to the way risks are treated in ISO/IEC 27001:2013.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the IT asset management system.

The organization shall provide the resources required for meeting the IT asset management objectives and for implementing the activities specified in the IT asset management plan(s).

7.2 Competence

The organization shall:

— determine the necessary competence of person(s) doing work under its control that affects its IT asset performance, IT asset management performance and IT asset management system performance;

— ensure that these persons are competent on the basis of appropriate education, training, or experience;

— where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;

— retain appropriate documented information as evidence of competence; and

— periodically review current and future competency needs and requirements.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the re-assignment of currently employed persons; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control, who can have an impact on the achievement of the IT asset management objectives, shall be aware of:

— the IT asset management policy;

— their contribution to the effectiveness of the IT asset management system, including the benefits of improved IT asset management performance;

— their work activities, the associated risks and opportunities and how they relate to each other; and

— the implications of not conforming with the IT asset management system requirements.

7.4 Communication

The organization shall determine the need for internal and external communications relevant to IT assets, IT asset management and the IT asset management system including:

— on what it will communicate;

— when to communicate;

— with whom to communicate; and

— how to communicate.

7.5 Information requirements

The organization shall determine its information requirements to support its IT assets, IT asset management, IT asset management system and the achievement of its IT asset management objectives and organizational objectives. Requirements may include, but are not limited to financial, purchase, contract, license, technical, and organization information. In doing this:

a) the organization shall include consideration of:

— the significance of the identified risks;

— difficulty of controlling the characteristics of IT assets as described in Annex C.

— the roles and responsibilities for IT asset management;

— what measurements are needed for determining that the IT assets achieve what is expected of them in relation to the organization's overall objectives

— the IT asset management processes, procedures and activities;

— the exchange of information with its stakeholders, including service providers;

— the impact of quality, availability and management of information on organizational decision making;

b) the organization shall determine:

— the attribute requirements of identified information;

— the quality requirements of identified information;

— how and when information is to be collected, analysed and evaluated;

c) the organization shall specify, implement and maintain processes for managing its information;

d) the organization shall determine the requirements for alignment of financial and non-financial terminology relevant to IT asset management throughout the organization; and

e) the organization shall ensure that there is consistency and traceability between the financial and technical data and other relevant non-financial data, to the extent required to meet its legal and regulatory requirements while considering its stakeholders' requirements and organizational objectives.

7.6 Documented information

7.6.1 General

The organization's IT asset management system shall include:

— documented information as required by this document;

— documented information for applicable legal and regulatory requirements; and

— documented information determined by the organization as being necessary for the effectiveness of the IT asset management system, as specified in 7.5.

NOTE 1 The extent of the documented information for an IT asset management system can differ from one organization to another due to:

— the size of organization and its type of activities, processes, products and services;

— the complexity of processes and their interactions;

— the competence of persons;

— the complexity of the IT asset(s); and

— the need to be able to demonstrate compliance, e.g. with licensing terms and conditions.

NOTE 2 Sub-clause 7.5 is concerned with the determination of overall IT system requirements, which is an initial task associated with the development of an IT Asset Management system, although it needs to be reviewed periodically. Sub-clause 7.6 is concerned with a specific subset of that information, for the purpose of having reviewable information, i.e. audit trails.

7.6.2 Traceability of ownership and responsibility

Ownership and responsibility for all IT assets shall be documented information.

NOTE 1 Documentation of ownership and responsibility can exist at any level of detail or generality as the organization considers appropriate. Where there are mixed ownerships and responsibilities, such as for end-user devices and servers; and for software and data on that equipment, more granularity of documented information will typically be needed.

NOTE 2 Ownership of and responsibility for one type of IT asset can create a responsibility for a different type of IT asset. For example, a cloud service provider can create a significant licensing exposure if it adds cores to a cloud server which is providing Infrastructure-as-a-Service to a client organization.

7.6.3 Audit trails of authorizations and execution of authorizations

All authorizations shall be documented information. The documented information shall include details of (a) who made the authorization, (b) when, and (c) reason(s) why the authorization was given.

NOTE 1 There is no requirement for any specific types of authorization to exist, unless otherwise specified in this document. Authorizations can exist at any level of detail or generality as the organization considers appropriate. For example, authorizations can apply to the entire organization, to specific organizational units or groups of individuals, to individual IT assets or classes of IT assets. Authorizations can also be time-limited. Furthermore, there can be different classes of authorizations, such as financial, security, operational, and managerial.

The execution of an authorization should be documented information, including details of (a) who executed it, (b) when it was executed, and (c) against which authorization(s).

NOTE 2 An example of the execution of an authorization is the installation of authorized software.

7.6.4 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

— identification and description (e.g. a title, date, author, or reference number);

— format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

— review and approval for suitability and adequacy.

7.6.5 Control of documented information

Documented information required by the IT asset management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

— distribution, access, retrieval and use;

— storage and preservation, including preservation of legibility;

— control of changes (e.g. version control); and

— retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the IT asset management system shall be identified, as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 6.1, the IT asset management plan(s) determined in 6.2, and the corrective and preventive actions determined in 10.1 and 10.2 by:

— establishing criteria for the required processes;

— implementing the control of the processes in accordance with the criteria;

— keeping documented information to the extent necessary to have confidence and evidence that the processes have been carried out as planned; and

— treating and monitoring risks using the approach described in 6.1.3.

8.2 Management of change

Risks associated with any planned change, permanent or temporary that can have an impact on achieving the IT asset management objectives, shall be assessed before the change is implemented.

The organization shall ensure that such risks are managed in accordance with 6.1.3.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

8.3 Core data management

The organization shall ensure that required data about all core IT assets in scope is accurately recorded throughout the life cycle; and that there is documented information for all IT assets as to whether they are authorized or not.

NOTE 1 Core IT assets include software assets, IT hardware, and IT asset services. Digital information content assets (e.g. licensed audio and video recordings; word-processing and PDF documents) are also considered core IT assets if they are included in scope. In situations with mixed responsibilities (e.g. for cloud computing or BYOD), it can be appropriate to include assets which are the responsibilities of other organizations or individuals in order to manage related risks, e.g. of licensing non-compliance.

NOTE 2 This process includes data verification.

NOTE 3 This process provides information on IT assets to support the effectiveness and efficiency of other business processes.

8.4 License management

The organization shall ensure that required data and information about licenses, related entitlements, and usage against entitlements, for all IT assets in scope, is accurately recorded throughout the life cycle; that reconciliations are conducted and assessed periodically between requirements, usage against entitlements, and entitlements; and verified.

NOTE If digital information content assets are included in scope and are subject to licensing terms and conditions, they would also be covered by these requirements.

8.5 Security management

The organization shall manage security effectively within all ITAM activities and shall support the security approval requirements related to ITAM, for all IT assets in scope; and conduct periodic verification of compliance with security requirements.

NOTE Security includes access and integrity controls. Security requirements apply not only to software but to all IT assets including hardware and information about IT assets.

8.6 Other processes

The organization shall ensure the operation of any other processes as determined in 6.2.2 *IT asset management objectives for operation processes*, and any additional processes which the organization has defined.

NOTE This sub-clause is the mechanism to add additional processes as defined in Annexes A and B.

8.7 Outsourcing and services

When the organization outsources any activities that can have an impact on the achievement of its IT asset management objectives, it shall assess the associated risks. The organization shall ensure that outsourced processes and activities are controlled.

NOTE 1 Outsourced activities in principle include externally supplied services. Examples of externally supplied services are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), as well as hardware maintenance, software support, and training. However, the term outsourcing is generally applied to relatively comprehensive sets of services, whereas individual services are generally considered more limited in scope.

NOTE 2 See ISO/IEC 20000-1 for further information on managing outsourcing and services.

When the organization utilizes an IT infrastructure with responsibilities for IT assets or data and information shared by both the internal organization and external suppliers of IT services, the organizations shall assess the associated risks. The organization shall ensure that processes and IT infrastructure involving mixed responsibilities are controlled.

NOTE 3 Examples of situations involving mixed responsibilities are that different parties can own the end-user devices being used (organizational vs third party such as a mobile operator), the servers being used (organizational vs third-party such as for cloud computing), the software being licensed (organizational or third-party), and the data being held and processed (organizational, personal, or third-party).

The organization shall determine and document how these activities will be controlled and integrated into the organization's IT asset management system. The organization shall determine:

a) the processes and activities that are to be outsourced (including the scope and boundaries of the outsourced processes and activities and their interfaces with the organization's own processes and activities);

b) the implications of the mixed responsibilities involved (including the associated risks and how the mixed responsibilities can be effectively discharged with accountability for those responsible);

c) the responsibilities and authorities within the organization for managing the outsourced processes and activities; and

d) the processes and scope for the sharing of knowledge and information between the organization and its contracted service provider(s).

When outsourcing any activities, the organization shall ensure that:

— the outsourced resources meet the requirements of 7.2, 7.3 and 7.6; and

— the performance of the outsourced activities is monitored in accordance with 9.1.

8.8 Mixed responsibilities between the organization and its personnel

When there is mixed ownership between the organization and its personnel of IT assets in scope and information held on those assets, it may have an impact on the achievement of the organization's IT asset management objectives. Where this is the case, the organization shall assess the associated risks and ensure that these situations are controlled.

NOTE 1 Situations involving mixed ownership between the organization and its personnel include personnel using their own devices for organizational activity (typically referred to as 'Bring-Your-Own-Device', or 'BYOD'), and also personnel using organizational IT assets for personal purposes, including the result that personal data or information can be held on organizational resources.

When the organization utilizes an IT infrastructure with mixed responsibilities between the organization and its personnel for IT assets or data or information, the organizations shall assess the associated risks. The organization shall ensure that processes and IT infrastructure involving such mixed responsibilities are controlled.

NOTE 2 Examples of situations involving mixed responsibilities are that different parties can own the end-user devices being used (organizational vs personal or third party such as a mobile operator), the software being licensed (organizational, personal, or third-party), and the data or information being held and processed (organizational, personal, or third-party).

The organization shall determine and document how these activities will be controlled and integrated into the organization's IT asset management system. The organization shall determine:

a) the processes and activities that are affected by mixed responsibilities between the organization and its personnel (including the scope and boundaries of the affected processes and activities);

b) the implications of the mixed responsibilities involved (including the associated risks and how the mixed responsibilities can be effectively discharged with accountability for those responsible);

c) the responsibilities and authorities within the organization for managing the situations involving mixed responsibilities; and

d) the processes and scope for the sharing of knowledge and information between the organization and its personnel in these situations involving mixed responsibilities.

When involved in situations involving mixed responsibilities, the organization shall ensure that:

— the mixed-responsibility resources meet the requirements of 7.2, 7.3 and 7.6; and

— the performance of the mixed-responsibility activities is monitored in accordance with 9.1.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

a) what needs to be monitored and measured;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

c) when the monitoring and measuring shall be performed; and

d) when the results from monitoring and measurement shall be analysed and evaluated.

The organization shall retain appropriate documented information as evidence of the results of monitoring, measurement, analysis and evaluation.

The organization shall evaluate and report on:

— the IT asset performance;

— the IT asset management performance, including financial and non-financial performance; and

— the effectiveness of the IT asset management system.

The organization shall evaluate and report on the effectiveness of the processes for managing risks and opportunities.

The organization shall ensure that its monitoring and measurement enables it to meet the requirements of 4.2.

9.2 Internal audit

9.2.1 The organization shall conduct internal audits at planned intervals to provide information to assist in the determination on whether the IT asset management system:

a) conforms to:

— the organization's own requirements for its IT asset management system;

— the requirements of this document; and

b) is effectively implemented and maintained.

9.2.2 The organization shall:

a) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting, which shall take into consideration the importance of the processes concerned and the results of previous audits;

b) define the audit criteria and scope for each audit;

c) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

d) ensure that the results of the audits are reported to relevant management; and

e) retain documented information as evidence of the results of the implementation of the audit programme and the audit results.

9.3 Management review

Top management shall review the organization's IT asset management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the IT asset management system;

c) information on the IT asset management performance, including trends in:

— nonconformities and corrective actions;

— monitoring and measurement results;

— audit results;

d) IT asset management activity;

e) opportunities for continual improvement; and

f) changes in the profile of risks and opportunities.

The outputs of the management review shall include decisions related to continual improvement opportunities and any need for changes (see 8.2) to the IT asset management system.

The organization shall retain documented information as evidence of the results of management reviews.

10 Improvement

10.1 Nonconformity and corrective action

When a nonconformity or incident occurs in its IT assets, IT asset management or IT asset management system the organization shall:

a) react to the nonconformity or incident, and, as applicable:

   — take action to control and correct it;

   — deal with the consequences;

b) evaluate the need for action to eliminate the cause(s) of the nonconformity or incident, in order that it does not recur or occur elsewhere, by:

   — reviewing the nonconformity or incident;

   — determining the causes of the-nonconformity or incident;

   — determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes (see 8.2) to the IT asset management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities or incident encountered.

The organization shall retain documented information as evidence of:

— the nature of the nonconformities or incident and any subsequent actions taken; and

— the results of any corrective action.

10.2 Preventive action

The organization shall establish processes to proactively identify potential failures in IT asset performance and evaluate the need for preventive action.

When a potential failure is identified the organization shall apply the requirements of 10.1.

10.3 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of its IT asset management and the IT asset management system.

Annex A
(normative)

IT asset management operation processes and objectives

This annex specifies the IT asset management operation processes and objectives which shall be considered for inclusion in the IT asset management system. The Statement of Applicability (6.2.2) documents the decisions as to which are included or excluded.

This annex is referenced or used in the main body of this document as follows:

— 6.2.1 IT asset management operation process specification;

— 6.2.2 IT asset management objectives for operation processes;

— Clause 8 Operation including in particular:

  — 8.2 Management of change;

  — 8.3 Core data management;

  — 8.4 License management;

  — 8.5 Security management; and

  — 8.6 Other processes.

Note that the process objectives for the first four processes are already included in this document, and consequently shall always be included (8.2, 8.3, 8.4, and 8.5).

Process types are either life cycle or functional. Life cycle management processes are those which reflect stages in the life cycle of the IT assets themselves. Examples are Acquisition, Release, and Deployment. Functional management processes in contrast generally apply across multiple life cycle processes (and hence the term 'cross-cutting' processes is sometimes used). Examples are Change Management, License Management, and Relationship and Contract Management.

Figure A.1 gives an overview of the process areas by process type.

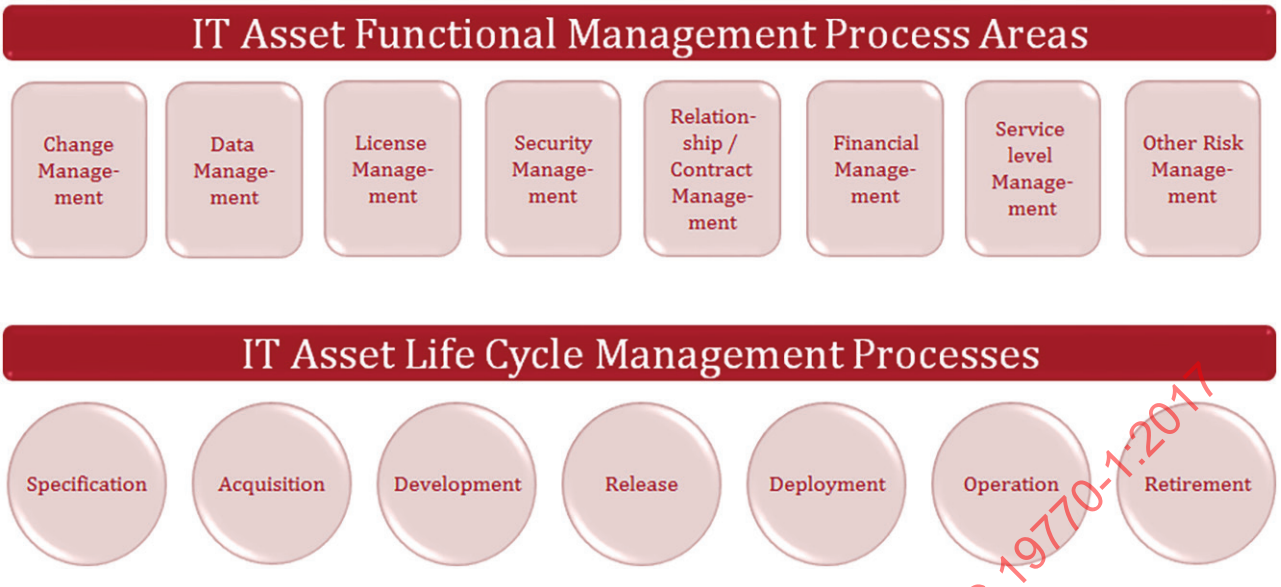

Figure A.1 — ITAM process areas by process type

Table A.1 gives the detailed process objectives structured by process type.

Table A.1 — Process objectives by process type

Process	Process Objective
IT Asset Life Cycle Management Processes	
Specification	The objective of the Specification process in respect of IT assets is to ensure that requirements are properly requested and analysed, and that appropriate alternatives are designed and evaluated for meeting those requirements.
Acquisition	The objective of the Acquisition process in respect of IT assets is to ensure that assets in scope are acquired in a controlled manner and properly recorded.
Development	The objective of the IT development process in respect of IT assets is to ensure that IT assets in scope, and software in particular, is developed in a way which considers ITAM requirements.
Release	The objective of the IT asset release management process in respect of IT assets is to ensure that releases of IT assets in scope are planned and executed in a way which supports ITAM requirements.
Deployment	The objective of the IT asset deployment process in respect of ITAM is to ensure that the deployment and redeployment of IT assets in scope is executed in a way which supports ITAM requirements.
Operation	The objective of the IT asset operations process in respect of ITAM is to ensure that operational processing utilizing IT assets in scope is executed in a way which supports ITAM requirements. NOTE The Operation process which is performed both by end-users and operators includes use of IT assets (e.g. taking backups and other 'housekeeping' tasks); monitoring (e.g. for exception conditions; and also of usage and performance); and optimization (e.g. adjusting configuration parameters to improve performance or cost-effectiveness). There is considerable integration with other ITAMS requirements. For example, compliance with acceptable use policies integrates with this process. Many of the IT asset functional management processes will integrate with this process, such as license management, to optimize the deployment of licenses.