UNIVERSITY OF VAASA

FACULTY OF TECHNOLOGY

SOFTWARE ENGINEERING

Anton Pääkkönen

ASSET MANAGEMENT IN AN ICT COMPANY USING ISO/IEC 19770

Master's thesis for the degree of Master of Science in Technology submitted for inspection, Vaasa, 25 September 2017.

Supervisor	Prof. Jouni Lampinen
Instructor	M.Sc. (Tech.) Olli Rajala

PREFACE

"Asset Management in an ICT Company Using ISO/IEC 19770" has been an almost a year-long project for me, and we still have some work to be finished at Wapice Ltd. Doing a research of the topic and being able to write the Master's thesis about it has been a great opportunity, challenge and an educator for me. At the point of adding my last words to the work I can be content with the outcome.

I would like to thank my supervisor Professor Jouni Lampinen and instructor M.Sc. (Tech.) Olli Rajala for assisting me on the study whenever I needed.

I would like to thank my family and my girlfriend Annika for the continuous support and encouragement throughout my studies.

Vaasa, 14.9.2017

Anton Pääkkönen

TABLE OF CONTENTS

ABBREVIATIONS

API	*Application Programming Interface*, an interface for communication between software components
CMDB	*Configuration Management Database*, a repository for storing configuration items, such as IT assets
CMMS	*Computerized Maintenance Management System*, an application package behind the asset management of an enterprise
DIS	*Draft International Standard*, an abbreviation for an ISO standard in draft stage of development
ERP	*Enterprise Resource Planning*, a system for enterprises for managing the core business processes
ICT	*Information and Communications Technology*, covers all of the medias which can be used in electronic data processing
ISO/IEC	*International Organization for Standardization/International Electrotechnical Commission*, a mark of an item jointly developed between ISO and IEC
IT	*Information Technology*, the application of computers and telecommunications for processing data
ITAM	*IT Asset Management*, an organizational practice to gather information about IT assets to help managing the organization's systems
ITIL	*IT Infrastructure Library*, a framework of practices for managing the services of IT applicable for organizations
regid	*Unique Registration ID*, an unique identifier that organizations use to identify software developed by them in the form of URI
SAM	*Software Asset Management*, a set of ISO/IEC standards which includes the family of ITAM standards

SWID	*Software Identification*, an abbreviation used often with SWID tags used to record information about a software or related asset
UML	*Unified Modeling Language*, a modeling language used in software engineering to provide standardized visualization of a design
URI	*Uniform Resource Identifier*, a sequence of characters that identifies a resource
XML	*Extensible Markup Language*, a both human- and machine-readable, widely usable markup language for document encoding
XSD	*XML Schema Definition*, a standardized recommendation for how to describe the elements in an XML-file

UNIVERSITY OF VAASA
Faculty of technology
Author: Anton Pääkkönen
Topic of the Thesis: Asset Management in an ICT Company Using ISO/IEC 19770
Inspector: Prof. Jouni Lampinen
Instructor: M.Sc. (Tech.) Olli Rajala
Degree: Master of Science in Technology
Degree Programme: Degree Programme in Information Technology
Major of Subject: Software Engineering
Year of Entering the University: 2012
Year of Completing the Thesis: 2017 **Pages:** 99

ABSTRACT:

Asset management refers to a system which organizations use to manage the both objective and non-objective assets with an existing value. By doing so organizations can achieve better financial results through cost reductions, satisfy the customers better with stability and improve the knowledge management. However, because of the broad scope of demands included in a standardized level of asset management, achieving a good level of such a management is rarely achieved in a large scope.

This thesis aims to develop a guideline for an ICT company about how to achieve efficient asset management for IT assets. The guideline is closely tied to the international ISO/IEC 19770 family of standards for IT asset management (ITAM). With standardized ITAM, the ICT company can have a single-point life cycle management source to provide various advantages in a long-term stability. To achieve general advantage, the set research question is "how an ICT company can achieve the ISO/IEC 19770 level of ITAM?" The study is done using active research model in a close co-operation with a Finnish ICT company. As ISO/IEC 19770 consists of multiple parts, the limitation with the target company comes as a focus on the first five parts. The rest of the standard family's parts are covered in a more general level in this thesis.

The target company's current state was researched and completed with the asset management's theory. The study produced a guideline for how an ICT company can implement ITAM's best practices which are in conformance to the ISO/IEC 19770 standard family's parts. The guideline includes the description of the guideline, a description for a common scenario in a company with common management errors, the proposed implementation for the ITAM, the benefits and liabilities, and the post-implementation steps. As the standards can be achieved in parts, the company can achieve the parts by following the guideline and the related requirements. The results of the study suggest, that a careful planning, designing and a continuous observance to the related processes are essential for achieving the best-in-class ITAM. The target company may continue the work from here by implementing the practices according to the proposed implementation guideline.

KEYWORDS: Enterprise asset management, ITAM, ISO/IEC 19770

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Anton Pääkkönen
Tutkielman nimi: Omaisuudenhallinta ICT-alan yrityksessä ISO/IEC 19770:n avulla
Valvojan nimi: Professori Jouni Lampinen
Ohjaajan nimi: DI Olli Rajala
Tutkinto: Diplomi-insinööri
Koulutusohjelma: Tietotekniikan koulutusohjelma
Oppiaine: Ohjelmistotekniikka
Opintojen aloitusvuosi: 2012
Tutkielman valmistumisvuosi: 2017 **Sivumäärä:** 99

TIIVISTELMÄ:

Omaisuudenhallinnalla viitataan järjestelmään, jolla organisaatiot voivat hallinnoida sekä aineellisia että aineettomia omaisuuksia, joilla on jokin arvo. Tekemällä näin organisaatiot voivat saavuttaa parempia taloudellisia tuloksia kustannusvähennyksillä, tyydyttää asiakkaitaan paremmin vakaudellaan sekä parantaa organisaation tietohallintoa. Kuitenkin, standarditason omaisuudenhallinnan asettamien kattavien vaatimusten takia, korkean tason hallinnointia harvoin saavutetaan isossa mittakaavassa.

Tämä diplomityö pyrkii kehittämään suosituksen ICT-alan yritykselle siitä, miten yritys voi saavuttaa IT-omaisuuksien tehokkaan hallinnoinnin. Suositus on läheisesti sidoksissa IT-omaisuuksien hallinnoinnin (ITAM) kansainväliseen ISO/IEC 19770 -standardiperheeseen. Standardoidun ITAM:n avulla yrityksellä voi olla yhden pisteen elämänkaarihallinnoinnin lähde tuottamaan moninaisia, pitkäaikaista vakautta edistäviä etuja. Yleisen hyödyn saavuttamiseksi työssä on asetettu tutkimuskysymys ”kuinka ICT-alan yritys voi saavuttaa ISO/IEC 19770 -tason ITAM:n?” Tutkimus on tehty toimintatutkimuksen menetelmällä läheisessä yhteistyössä suomalaisen ICT-alan yrityksen kanssa. Koska ISO/IEC 19770 koostuu useista osista, muodostuu näistä rajaus työn keskittyessä kohdeyrityksen tapauksessa standardiperheen viiteen ensimmäiseen osaan. Standardiperheen muut osat käsitellään työssä yleisemmällä tasolla.

Kohdeyrityksen nykytilaa tutkittiin ja tietoja täydennettiin omaisuudenhallinnoinnin teorian avulla. Tutkimus tuotti ohjeistuksen siitä, miten ICT-alan yritys pystyy toteuttamaan ITAM:n parhaat käytännöt ISO/IEC 19770 -standardiperheen mukaisesti. Ohjeistukseen sisältyy ohjeistuksen kuvaus, yrityksen yleisen tilanteen kuvaus yleisine hallinnointivirheineen, ITAM:n ehdotettu toteutustapa, hyödyt ja velvoitteet, sekä toteutuksen jälkeisten työvaiheiden kuvaus. Koska standardit voidaan saavuttaa osissa, yritys voi saavuttaa osat noudattamalla ohjeistusta ja niihin liittyviä vaatimuksia. Tutkimuksen tuloksien perusteella voidaan todeta, että huolellinen suunnittelu ja työhön liittyvien prosessien jatkuva noudattaminen ovat välttämättömiä parhaimman tason ITAM:n saavuttamiseksi. Kohdeyritys voi jatkaa työtä tästä toteuttamalla työvaiheet ehdotetun toteutustavan mukaisesti.

AVAINSANAT: Yrityksen omaisuudenhallinta, ITAM, ISO/IEC 19770

1 INTRODUCTION

In the world of enterprises, asset management means a system, which organizations can use to manage the life cycle of both objective and non-objective assets having some value. Assets, the primary objects of asset management, are any items, things or entities which have an existing value and are owned by someone (Davis 2012: 6; The Institute of Asset Management (IAM) 2015: 8). The aim of the asset management system is to utilize assets of the enterprise at the most efficient level. Doing so, organizations can achieve better financial results via cost reductions, satisfy their customers better and improve the organization's information management (Mohseni 2003: 962–963; Kumar & Suresh 2007: 215; Hastings 2010: 4–5; Lin, Lan, Ye & Wu 2013: 456). However, because of the broad scope of demands included in a standardized level of asset management, achieving a good level of such a management requires a significant amount of work and co-operation from the organization (Helstrom & Green 2011: 353; Lin *et al*. 2013: 456–458).

1.1 Research Background and Motivation

The study is done as an assignment to a Finnish software company Wapice Ltd. while the author has been working in the company. Wapice Ltd. has been established in 1999 in Vaasa, and the company employees around 320 people (situation at 12/2016) (Wapice 2016). The employees hold by basis several assets owned by the company, such as a computer, its hardware and the software used in the computer. As the company operates at multiple locations, the assets are also spread to different locations. Because of this, the tracing and maintaining of the assets becomes more complicated, and a need for an efficient way to manage assets has emerged.

Prior to the study the tracing and maintaining of the assets has been done using several systems, which some of them have not been integrated to each other. Some of the systems require a manual input from an administrative person which affects the performance of administration. To save time and to better support the users in need of assistance in terms of time and quality, a centralized and more automatized system should be developed. In

order to develop a well-designed system which comprehensively covers the both objective and non-objective assets, the development should be based on the related standards of IT asset management.

1.2 Research Goal and Question

This thesis aims to develop a designed guideline about how the company can achieve the maintaining of the IT assets most efficiently. This guideline works as a suggestion about whether the company should pursue the most efficient IT asset management and how to do that. The guideline is strongly tied to an international family of standards for IT asset management (*ITAM*), ISO/IEC (*International Organization for Standardization/International Electrotechnical Commission*) 19770. With standardized ITAM it is possible to develop a single-point life cycle management source as a system. This system will be based on the already existing configuration management database (*CMDB*) part of the company's IT infrastructure library (*ITIL*). The CMDB as a system can be used to achieve multiple advantages in the long-term stability of the company's IT assets. As a research the study attempts to answer the set research question "*how an ICT company can achieve the ISO/IEC 19770 level of ITAM?*" For how the study will be done is defined in more detail in chapter 1.3.

As a limitation for the study will be that only IT assets of enterprise assets are considered. Furthermore, as the family of standards in question, ISO/IEC 19770, is actively under development, the study will only focus on the parts 19770-1–19770-5. Of these parts the 19770-4 is a DIS (*Draft International Standard*) published on October 21, 2016, at the stage of enquiry with an ongoing DIS ballot (ISO/IEC DIS 19770-4 2016; ISO 2016). The guideline developed for the target company covers the parts 19770-1–19770-5, but excludes the upcoming standards.

1.3 Structure

There can be seen two main parts in the thesis. The first part of the thesis defines the theory of the study. The theory consists of the definition of asset management and especially ITAM by a general definition and by the ISO/IEC 19770 family of standards. The second part of the study is about developing the ITAM suggestion for the target company. This part covers also the answering to the set research question. In general the study proceeds in a feasible order so that each part's theory is elaborated before its possible practical covering.

The theoretical part of the study is done as a literature review. The general definition of asset management and what it means in IT terms is précised by the literature of Bonham (2004) and Hastings (2010) and by several articles concerning asset management. The covered standards of ISO/IEC 19770 are defined by the original papers of the standards available at 12/2016.

The more practical part of the study, which is done in a co-operation with the target company, is done in the form of *action research*. By the definition of action research the study attempts to both solve a problem (the ITAM guideline for the target company) and to produce scientific results (the answer to the research question). The action research is started by at first determining the current state at the target company, which will work as a basis for the guideline. After this the guideline is developed and afterwards evaluated. As the process in action research is iterative, the process is then repeated (Koshy 2005: 3–10). However, in this study the results are collected from the first iteration of the action research.

2 ASSET MANAGEMENT

To understand what asset management is for, it is important to understand what assets are. Assets are any items, things or entities which have an existing value. Assets may be either objective or non-objective, meaning they do not have to physically exist. Another descriptive characteristic is that assets are owned by someone – an individual or a corporation (Davis 2012: 6; IAM 2015: 8). The value, or potential in certain scenarios, of assets is something determined by the assets' owner. The value comes from the significance of the asset, without which the enterprise's ability to support its customers or its own performance suffers, and from the asset's purely financial value (Green & Helstrom 2011: 364). An individual asset does not necessarily have a significant value. Instead the value of an asset may only be valid when the asset is connected to a larger entity (IAM 2015: 11).

Hastings (2010: 3) divides assets into two types: *fixed* assets and *current* assets. Fixed assets are assets which have a value over a period of one year. Examples of fixed assets are buildings and machinery. Current assets are described as faster moving assets such as materials in inventories and cash. If an asset is assumed to be on the record for longer than one year, it is labeled as a fixed asset. Thus in this thesis the assets in question are fixed assets.

Asset management is not necessarily only for enterprises as its practices may also be applied to individuals (Davis 2012: 6). However, in this thesis the focus is on the former. The chapters 2.1 and 2.2 define the theory of asset management in enterprise context with a focus on ITAM. The definition is based on a literature review of enterprise asset management and its subfields.

2.1 Enterprise Asset Management

For businesses, asset management is an important, but complex practice to realize the value of assets in a coordinated manner (IMA 2015: 8). The cyclic process of asset management, as seen on Figure 1, often refers to the operating and managing of the assets, but also the deploying, maintaining, upgrading and disposing of the assets are fundamental elements of the process (Hastings 2010: 4; Davis 2012: 7–12). Effectively managed asset management will involve multidisciplinarily various branches of an organization such as finance and engineering (Frolov, Ma, Sun & Bandara 2010: 19; Davis 2012: 7). Despite the ability to integrate into large, multinational enterprises, asset management suits for all organization types whether they are governmental, non-profit organizations or for example small, privately owned businesses (Barry, Helstrom & Potter 2011: 110; IAM 2015: 8).

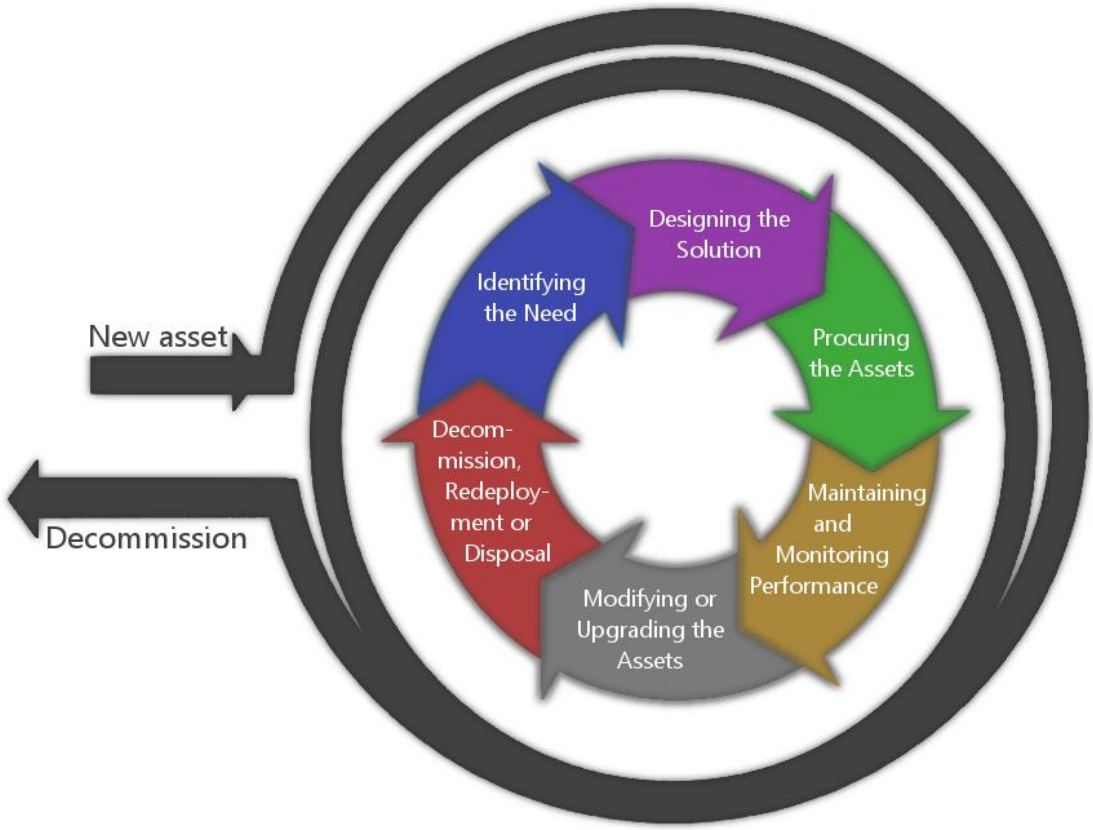


Figure 1. Assets have a cyclic life course. (Restructured from Zutec 2016.)

The need for asset management comes from several factors. Assets age and become outdated; their owners and physical locations change; support cases arise where the history and details of the assets are needed; and for financial and security managing purposes the assets need to be managed (Frolov *et al.* 2010: 20). Enterprises do not only want to solve the problem points, but also improve their current practices. Economies aim to identify the maximal profit-returning assets with cost/benefit-evaluation, infrastructure's life cycle costs need to be managed to spot the points for improvements and possibilities to extend the life of assets of both fixed and current assets (Barry *et al*. 2011: 90; Davis 2012: 4). Correctly managed the enterprise asset management becomes a tool for better service and up-time for assets (Barry *et al.* 2011: 110). It may also improve the organization's reputation, ability to fulfill the organization's obligations, operability safeness, business strategy evaluation and even the cost of the actual asset management (IAM 2015: 8).

Asset management in practice should do most of the asset-related decisions by its rules. For assets critical to the organization, specific rules and strategies can be defined as a failure-preventive practice. The preventative maintenance should cover the assets' time-, condition- and usage-based properties (IAM 2015: 45). Generally when an asset's planned replacement would cost less, in terms of time and consequential losses, than an unplanned replacement, it is recommended to replace the assets according to a timed plan instead of on a failure (IAM 2015: 44). However, each warning, error and failure triggering an alarm needs to be examined by a professional. An organization should be aware that a strict economy-policy may cause obvious end-of-life incidents (IAM 2015: 44). That said, it becomes organization's responsibility to find a balance between reliability versus operating and maintenance costs.

To be an authoritative source of information, asset management needs to be managed by the organization's senior-level manager. From the manager this requires visible leadership and commitment, but both of these characteristics should also be demonstrated throughout the organization's management levels. For the enterprise, authoritatively valued asset management system is able to offer consistent decision making. The decision making should take into account the asset's performance versus maintenance; investment

costs compared to operating expenses; and short-term benefits against the long-term sustainability. The final decision comes as a compromise from the competing interests. The complexity behind decision making varies, as does the criticality of the decision too. The decisions with several influences, options, timings or interdependencies should always be relied on the system. However, the simplest, non-critical decisions are allowed, and should be done by a professional with the use of common sense. (IAM 2015: 12–13 & 39.)

The today's way of asset management involves the use of a computerized maintenance management system (*CMMS*). CMMS offers the content to the asset management so that it essentially becomes the enabler of the asset management itself. The content, known as data, is the core of the CMMS. The data needs to be clearly defined and represent the core assets and their attributes thoroughly. These values, the enterprise wishes to store to the databases, should ultimately be hand-picked by people. CMMS's databases store the data about assets, which is further converted into primitive health information reports of the assets. For ITAM, a plain CMMS could be used for basic asset management, but to have the facilities for total enterprise asset management, a separate asset management system is required. This system, built to integrate CMMS amongst others, is many times required when the organization spans several geographical locations. (Barry *et al*. 2011: 90–92 & 105.)

As seen on Figure 2, enterprise asset management covers CMMS's fields in total, but also includes several financial and human resource management aspects. Enterprise resource management (*ERP*) systems of the organization cover most of the enterprise's asset management areas, but leave out the maintenance management – a core function of asset management. Maintenance management in its entirety incorporates modules for inventories, procurement, human resources, financials and general maintenance. In addition to these, the already rather complex maintenance management applications contain performance measurement, modern monitoring and reporting capabilities. (Barry *et al*. 2011: 91–92.)

The processes of enterprise asset management involves similar steps to what ITAM does involve. Because of this the processes of ITAM are only addressed in this thesis. This is

done in the chapter 2.2.1. As a consequence of similarity, the tools originally targeted for ITAM are often used to manage other assets too, and *vice versa* (Barry *et al.* 2011: 110; Green & Helstrom 2011: 367). The tools of ITAM are addressed in the chapter 2.2.2.

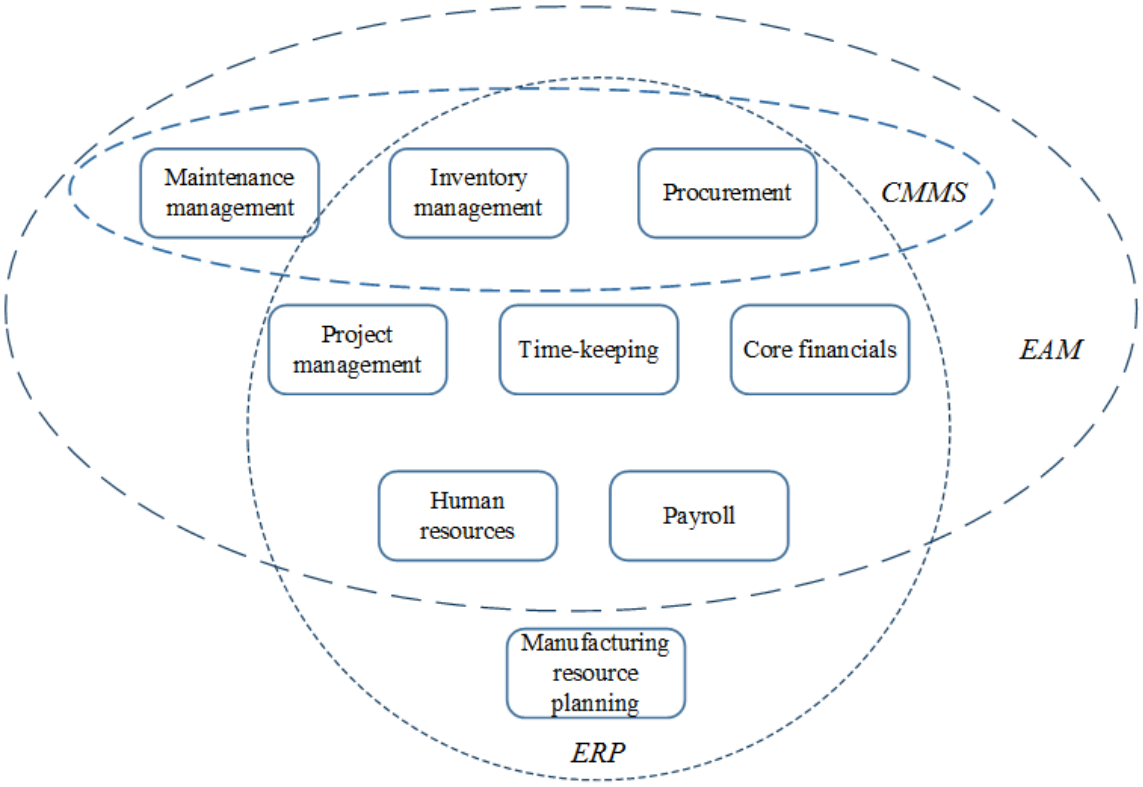


Figure 2. Comparison of CMMS (*computerized maintenance management system*), EAM (*enterprise asset management*) and ERP (*enterprise resource planning*). (Restructured from Barry *et al.* 2011: 92.)

2.2 IT Asset Management

ITIL in a total is a service-oriented practice extending the organization's uptime principles to provide IT services where needed. ITAM, being part of the ITIL process, in a high-level has many similarities in terms of actions and activities to the asset management which would apply to, for example, plant management. What explicitly differs ITAM is the terminology which better fits the nature of IT (Helstrom & Green 2011: 352 & 354–

355). Beyond that comes the more in-depth differences discussed in more detail on this chapter.

In the context of ITAM the assets are limited to the set of IT-specific objects, resources and non-objective items. IT assets have a common characteristic of providing value for the company through the services they enable. These assets could be thought as services supported by the IT team (Helstrom & Green 2011: 352). Bonham (2004: 21–22 & 150) divides the IT assets into 4 categories: hardware; software; contracts and licenses; and facilities. IT assets tend to have a relatively clear product life cycle. On the case of hardware, their value depreciates over time; software become outdated in terms of security, supportability and operability; contracts and licenses have an expiration date; and facilities have many of these characteristics shared by the hardware, software and contracts/licenses (Bonham 2004: 152). This simplifies the life cycle planning of IT assets, but at the same time marks the importance of ITAM.

In an organization with multiple units lies a recognized risk of the emergent of individual business silos. The silos control their own control process and assets in an unestablished way. Although locally things might work, the organization in total becomes immutable as its ability to adapt to changes is slowed down by decentralized management. Eventually the static organization cannot follow the pace of the markets affecting the enterprise's profitability and overall performance. This risk applies in particular to IT assets, such as systems, which should be able to integrate to each other without time-consuming challenges usually handled by the organization's IT team. With a centralized asset management process for IT assets this can be prevented. (Bonham 2004: 141–142.)

The centralized ITAM is often managed by the organization's IT team. This covers both the processes of the ITAM and the tools, which as highlighted by Helstrom & Green (2011: 355) should have a 4:1 ratio of focus in favor of processes. The IT team is expected to be in contact with the organization's purchasing-responsible unit. With a successful communication duplicate assets and thus unnecessary costs can be limited. Consequently the centralized purchasing process is yet another process which should be handled in a

centralized manner in the organization (Bonham 2004: 142). Regardless the fact that purchasing, often a visible sign in a process for the organization's members, goes through a process workflow and therefore causes a possible bottleneck, it undisputedly has its upsides in financial consideration. In addition, by centralizing the purchases, the organization may be able to gain benefits from the vendors in several ways. As the purchasing becomes centralized, the single purchasing unit becomes a more significant customer for the vendor often increasing the responsiveness. Also the procurement could possibly be simplified which could for example shorten the delivery times. Finally, in some cases it might be possible to negotiate for improved license terms and conditions (Bonham 2004: 152–153).

Besides financial purposes, which allow the organization to determine its total cost of ownership of the IT assets, there are two other core purposes for ITAM. Another core purpose is the operational aspect. IT's operational efficiency for the organization is a constantly monitored indicator, which should be able to provide seamless and rapid support for business-critical IT systems. ITAM enables the IT team to faster response and problem solving times. The third core purpose of ITAM is the support it provides for the enterprise's projects. For the purchase-responsible units this means, that they can ensure that the asset acquisition processes follow a unified guideline. For project management the ITAM can reduce the licensing and indirectly the training redundancy as well (Bonham 2004: 142–143).

A typical IT project consists of development, quality assurance and production environments. Additionally environments such as integration and training environments might be needed. Each environment involves various hardware, software and other related IT assets which all together sum up to notable costs. Over time, the involved assets tend to increase so, that the project accumulates more assets than is needed for a successful development. The assets recognized as excessive may become useful for example in the production use. However, not always a fitting reuse is found and the licenses of hardware and software become unused. Moreover, what happens to the assets once a project has finished one of its courses releasing the involved assets? (Bonham 2004: 145.)

2.2.1 ITAM Processes

The first step of ITAM's implementation is the development of the ITAM processes (Helstrom & Green 2011: 355). These ITAM processes, tied around the organization's ITIL, are to be developed one after another as they engage between each other. Helstrom & Green (2011: 356–357) mentions 4 processes to take into account at the beginning of ITAM's implementation. Each ITAM process is briefly covered below.

Configuration management is a process, which manages the identification, control, maintenance and verification of configuration items. Configuration items in ITAM's context are assets, but they could also refer to the business processes, collections and virtual resources. Configuration items are stored in a CMDB part of the organization's ITIL. The framework of configuration management consists of CMDB's setup; defining of configuration items; and defining and executing the discovery methods. If the CMDB is not already implemented in the organization's ITIL, its control and verification processes should also be developed. A functional configuration management in the other hand connects to existing CMDBs, supplies validated configuration items to the database and deploys the processing practices of configuration items throughout the enterprise. (Helstrom & Green 2011: 356.)

Incident management is a process, which aims to minimize the impact incidents may cause for the services and other related practices the organization carries out. This is done by preparing to incidents based on their symptoms and effects; by analyzing the causes; and by resolving the issues. In ITAM the incidents may be equipment failures, outages on services or unexpected discoveries of assets. Incident management's framework requires maintenance service functions in case of incidents, reporting triggers for incidents and an incident record. A functional incident management needs to be in a close relationship with configuration management and change management to track the origin, licensing, usage and maintenance history of each asset. (Helstrom & Green 2011: 356–357.)

Change management is a process, which controls and monitors the requests for change and their processes. In ITAM this concerns any change to the assets, but it may also concern changes to processes or to the organization. The framework of change management consists of a basic workflow for change request. To functionalize the change management, its workflows should be automated so that any change updates the related inventory through the configuration management. (Helstrom & Green 2011: 357.)

Financial management is a process, where the assets' funding, budgets, costs and returns of investments are managed and reported. Financial management's framework calls for facilities to financial reporting processes and relevant infrastructure so that the users can access the data relevant to them. In addition, the managed and reported financial properties of the assets are linked to the configuration items. A functional financial management is comprehensively and explicitly tied to the organization's asset management so that it automatically processes the financial effects and reporting which may result from incidents or changes to assets (Helstrom & Green 2011: 357.)

2.2.2 Tools

After the processes of ITAM are prepared, the ITAM's implementation can move to the part where the tools to enable ITAM are considered. The tools to manage ITAM can generally be the same used to manage the enterprise's other assets besides IT. However, tools particularly developed for the managing of IT assets can be used to enhance the task's fulfilling. Tools like this tend to integrate to a system so that the discovery of the assets can be done inside out for the whole domain (Green & Helstrom 2011: 367). As a deployed solution, tools can be used to configure restrictions if it is applicable to the environment (Green & Helstrom 2011: 368).

Hastings (2010: 244–245) lists several features the tools of asset management should be able to provide. These include asset register; routine maintenance lists and prompts; work requests; work order management; data logging; reports for estimating, costing, costs,

budgeting and budgetary; spare asset management; suppliers; purchasing; work procedures; planning and scheduling; personnel directory; work history; and management reports. Which of these are applicable for ITAM or for a particular environment is to be decided by the enterprise itself. The primary tool for ITAM might be a single CMMS with a comprehensive set of features (Hastings 2010: 245; Barry *et al*. 2011: 91). If some of the key features are not available out-of-the-box, it is more and more often made possible by the CMMS to build custom solutions to complete the set.

To develop the solutions, and to generally understand the principles behind the built-in features, it becomes important to understand the theory behind them. In the most complex cases, such as in optimization tasks, the outputs are based on an estimate received from a purely mathematical operation. Campbell, Jardine & McGlynn (2011) lists several models, figures and formulas to aid in this including the following:

A. Mean time to failure – a formula for life-expectancy of a component
B. Estimating the distribution – a two-method model to estimate a distribution of for example a tool based on either maximum likelihood or the least squares
C. Optimal number of assets to meet a workload – a model to find the optimization between for example virtual servers are their usage
D. Optimal interval between breakdown-preventive replacements of assets – a model to optimize the life cycle renewal of a physical asset family
E. Optimal breakdown-preventive replacement age of an asset – a model similar to D which applies single assets based on their age
F. Optimal inspection frequency – a model to find the minimum of downtime by optimizing the intervals of equipment inspection

Of the listed optimization operations, it is also possible to consider the technological improvement from finite to infinite timespans, or to minimize a total cost based on multiple factors. (Campbell, Jardine & McGlynn 2011: 401–445.)

2.2.3 Inventories

To avoid the black hole of untracked IT assets, an inventory for IT assets should be established. The first part, and also the most challenging part of the establishing is to get a handle of the existing IT assets to the IT asset portfolio (Bonham 2004: 142–143; Helstrom & Green 2011: 353). The IT asset portfolio is to determine which assets should be managed by the ITAM (Bonham 2004: 21). This task should be done by the executives of the organization based on the criteria of maximization, balance and strategic alignment (Bonham 2004: 16). Of these, maximization means the best outcome based on the changing requirements set by the projects; balance means the relative proportioning of IT assets based on the need against capability; and strategic alignment means that the IT assets are relevant to the organization's strategy (Bonham 2004: 16–20).

After the IT asset portfolio has been conducted and implemented, the first inventories, known as *static inventories*, can be established (Bonham 2004: 143; Helstrom & Green 2011: 353). The inventories store the data of an organization's different sectors, segments, divisions or similar branch defined by the organization's strategy. Examples of these are manufacturing, financial, human resources and marketing inventory, but for a consistent organization a single inventory might suit the best (Bonham 2004: 145).

Setting up the static inventory follows the process of configuration management described in the chapter 2.2.1. Consequently, as seen on Figure 3, the inventories become the CMDB by consolidating the inventories, and the IT assets become the database's configuration items. However the assets registered at CMDB need to follow the other processes of ITAM too: incident management, change management and financial management (Bonham 2004: 145). This means that the assets' financial properties and usage history is to be collected to the static inventories as well according to their processes.

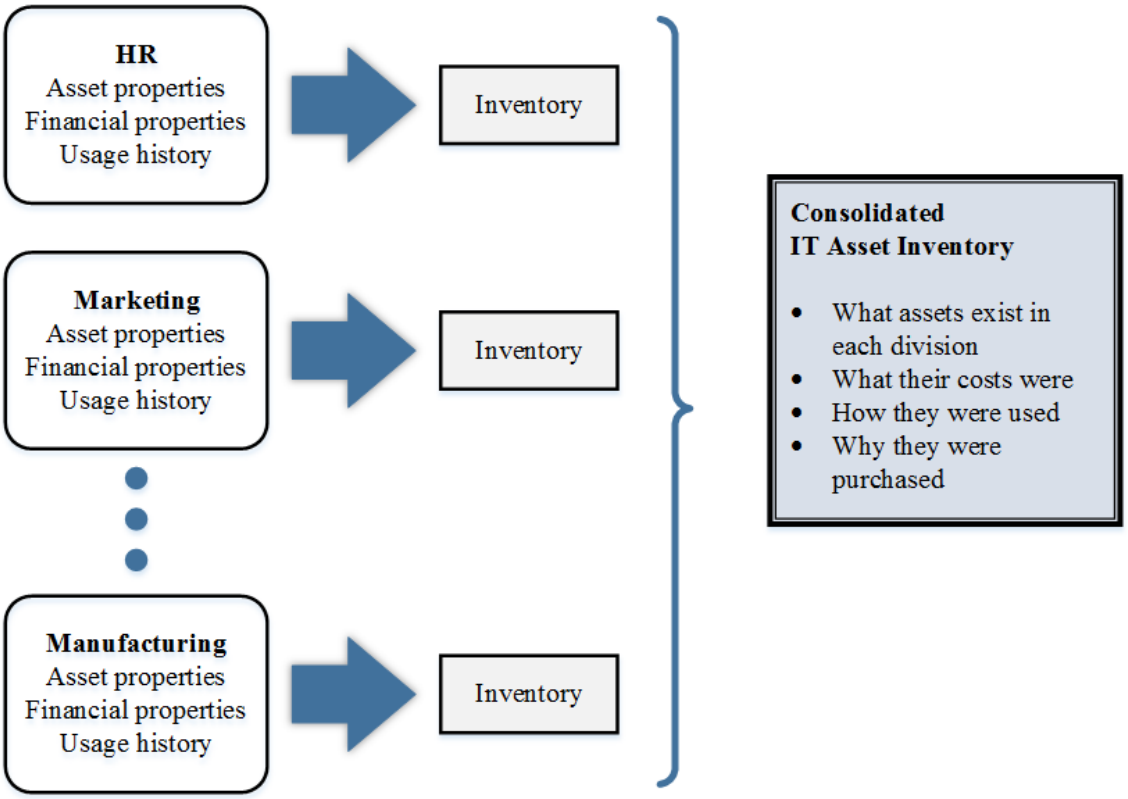


Figure 3. Inventories from the organization's different branches form the consolidated IT asset inventory. (Restructured from Bonham 2004: 145.)

The configuration items are to be collected with discovery methods, defined as part of the configuration management process, as extensively as possible. This not only automatizes the collection, but reduces the involvement from users, speeds up the process and greatly reduces the error-propensity. As automatized configuration item discovery at minimum requires a connection to the enterprise's domain, some of the assets need to be entered by hand. This is to be done either by the users by conducting surveys (Bonham 2004: 143), by collecting the data by assigned personnel, or by the mix of both. Operating at several geographical locations leads to moving assets, which may cause an increase at the discovery times (Bonham 2004: 143).

As the static inventories have been put into practice, the inventories need to be transformed into *dynamic inventories*. During the movement from static to dynamic, newly acquired assets need to be stored as during the forming of static inventory to prevent

future business silos occurring (Bonham 2004: 144). Dynamic inventories are the core enabler for functional configuration management. Their key feature is the precision by real-time provided by tools with auto-tracking features (Bonham 2004: 143 & 150–152). With an updated inventory the functionalized configuration management process feeds the CMDB with configuration items and furthermore makes the ITAM possible and its systems alive.

2.2.4 Challenges & Overcoming Them

While establishing the enterprise's ITAM system and familiarizing the organization to the involved processes, there are many challenges along the way. As ITAM's deployment in the organization progresses, a seemingly normal situations might already suggest an upcoming problem, so it is important to understand what such situations might be, how they are a problem and how to react to them. A well-designed ITAM is also well-planned and the challenges can be prevented already during the establishing. Some common challenges have been collected to below. While these assess several situations along the path to centralized ITAM, a specific risk management plan is recommended to have.

A typical organization has many sub-organizations: some for projects, some for units and some for people working inside the same domain. Sub-organizations are led, as for example projects have project managers, and the formation of a hierarchical unit with a unique purpose leads to a risk to cause the unit to become autonomous. Autonomously working unit might do approval-processes on its own, form an own stock or for example form hierarchy differentiating from the rest of the organization. These units, also known as silos, cause the organization to become immutable, as mentioned in the chapter 2.2. Besides that, it causes the asset management process to become spread out leading to multiple problems in asset management (Bonham 2004: 143–144). To control this, the organization needs to centralize the asset management. In addition, the purchasing workflows are to be tied as part of the asset management. This will require even more diligent management from the IT team which often does not show up to the end users (Bonham 2004: 145–146).

There are many pitfalls especially in managing the assets. This highlights the importance of forming the static inventory in a careful, thoroughly planned manner. Even with a carefully planned set up of static inventories, the IT team might face later a situation where there are excessive asset acquisitions (Bonham 2004: 152). Although this might offer more flexibility for stock management, it will also result in superfluous expenses. Commonly this is caused when the asset acquisition approvals are done at project-level. By doing the approvals at enterprise-level, the acquisitions will always go through the asset management system and prevent the issue from occurring (Bonham 2004: 152).

Other asset-related scenarios are that the assets are not effectively reused, assets with overlapping functions start to pile up and that assets become isolated. Lin *et al.* (2013: 457) suggest a *layered asset description framework* to resolve the challenges. The frameworks has the following three constituents:

1. Common description model: a description of an asset extracted from the shared features between different assets
2. Layered and typed description models: based on a four-layer-model (strategy, operation, execution, implementation), finding the assets in each layer and their type-specific unique characteristics as descriptions in the asset's layer
3. Semantical relationship: according to the types and layers of assets, semantically finding and designing both the intra- and inter-layer relationships between the assets. (Lin *et al.* 2013: 458.)

Layered asset description framework focuses to consider what an asset is by its own description and what metadata properties it has. Many of these properties become helpful when managing the asset's life cycle, whereas for example the asset type is useful in managing purposes. Transforming the framework to a machine readable format enables the relationships between assets so that assets can be found by their characteristics, the assets with overlapping features can be recognized and assets cannot become isolated. A one way to build the relationships between assets is illustrated on the Figure 4. (Lin *et al.* 2013: 458–459.)

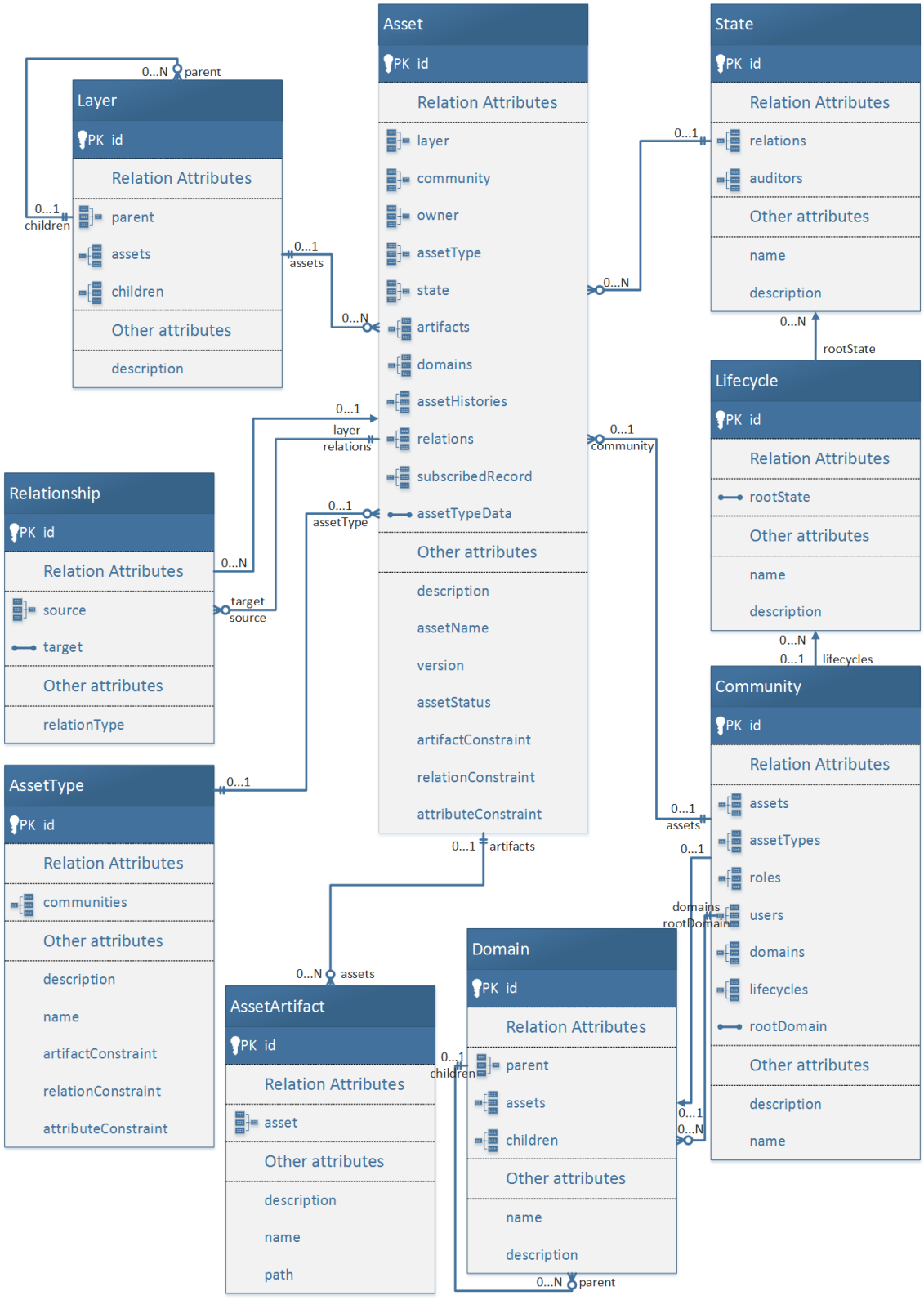


Figure 4. An example of layered assets' associations described in a database-format. (Re-structured from Lin *et al*. 2013: 459.)

2.2.5 Summary

IT assets follow the outline of the asset management's cyclic life course, which can be seen on chapter 2.1's Figure 1. IT assets, compared to the enterprise's other assets, have two significant differences: terminology and the relative shortness of the asset's life course. An IT asset part of the IT asset portfolio has seven different stages defined by the IT operations the asset will go through its life cycle. The seven IT asset-specific operations are the following:

1. Requisition – IT asset becomes requested for acquisition
2. Approval – The requisition becomes approved
3. Procurement – IT asset is purchased from a vendor
4. Receipt – The asset is received and handed to the IT team
5. Deployment – The asset is installed by the IT team and tested by the requester
6. Tracking – The asset's status is registered at ITAM by a discovery
7. Disposal – The asset is decommissioned. (Bonham 2004: 149–150; Green & Helstrom 2011: 364–365.)

Managing and optimizing the IT assets has a significant role on the business' cost-efficiency. This is achieved by minimizing the costs of assets and maximizing the return provided by the assets by following the ITAM's processes. The managing of IT assets, however, is a demanding challenge requiring continuous maintenance, service, support and planning to fulfill the task effectively (Green & Helstrom 2011: 363–364). In addition, several processes have been developed to aid on this task. These processes are part of the framework of ITIL (Green & Helstrom 2011: 366–367).

ITAM does not only set demands for the IT team managing the assets, but also for the rest of the organization. There are four principles which can guide the organization towards a unified, sustainable ITAM. The first principle is to reduce the tracking methods the organization already has aiming to one, completely covering method. The second principle is to standardize the processes of the organization with a bureaucracy-critic state of mind. As third, the IT assets need to be registered to the tool managing the tracking of

them. As fourth, and also as a primary goal, the ITAM needs to become a centralized source of information. (Green & Helstrom 2011: 364.)

3 ISO/IEC 19770

ISO/IEC 19770 is a family of standards for ITAM. The family consists of four standards which have reached the Publication-phase of a standard's life cycle and several standards and technical reports in different phases of development (ISO 2017a). The standards are listed on Table 1. The overview of the ITAM family of standards belongs to the scope of the standard ISO/IEC 19770-5 – Overview and vocabulary. However for sequencing reasons the covering of the family's overview is done in this chapter.

Table 1. Standards and technical reports which belong to the ISO/IEC 19770, a family of standards for ITAM, on 12/2016. (ISO/IEC 19770-5 2015: *iv* & 14–18; ISO 2017b.)

ISO number & part number	**Description**	**Life cycle phase**
ISO/IEC 19770-1	Processes and tiered assessment of conformance	90.92 Review
ISO/IEC 19770-2	Software identification tag	60.60 Publication
ISO/IEC 19770-3	Entitlement schema	60.60 Publication
ISO/IEC 19770-4	Resource utilization measurement	40.99 Enquiry
ISO/IEC 19770-5	Overview and vocabulary	60.60 Publication
ISO/IEC 19770-6	Embedded software tag	Planned
ISO/IEC 19770-7	Tag management	In development
ISO/IEC 19770-8	Guidelines for mapping of industry SAM practices with the ISO/IEC 19770 family of standards	30.20 Preparatory
ISO/IEC 19770-11	Guidelines for the application of ISO/IEC 19770-1 for small organizations	Planned
ISO/IEC 19770-22	Guidance for the use of 19770-2 software identification tag information in cyber security	In development

The family of standards for ITAM includes standards for different purposes. These purposes are the following:

- Process definition: processes, that enable demonstrating of organization's performance for effective software asset management (*SAM*).
- Implementation approach definition: approaches for implementing the processes of ITAM in a recognizable conformance-level.
- Information structure definition: information structures to support the processes of ITAM and to contain identification and management necessary information about a software.
- Additional information structure definition: information structures for asset management's specific functions, which can add details to the foundation information structures. (ISO/IEC 19770-5 2015: 14.)

Of the above mentioned purposes are formed the three categories of ISO/IEC 19770: Overview, Process and Information Structures. Information Structures category includes sub-categories for different functions, which are Software Identification, Entitlement, Usage, Device Identification and Tag Management. The categorizing of the ISO/IEC 19770 standards can be seen in Figure 5.

Figure 5 also distinguishes the actual standards from technical reports, although they all belong to the family of standards concept. Technical reports are to provide guidance for associated standards. As an example, technical report ISO/IEC 19770-22 is to support the standard ISO/IEC 19770-2 by giving guidance for software identification tag in cyber security context (ISO/IEC 19770-5 2015: 17).

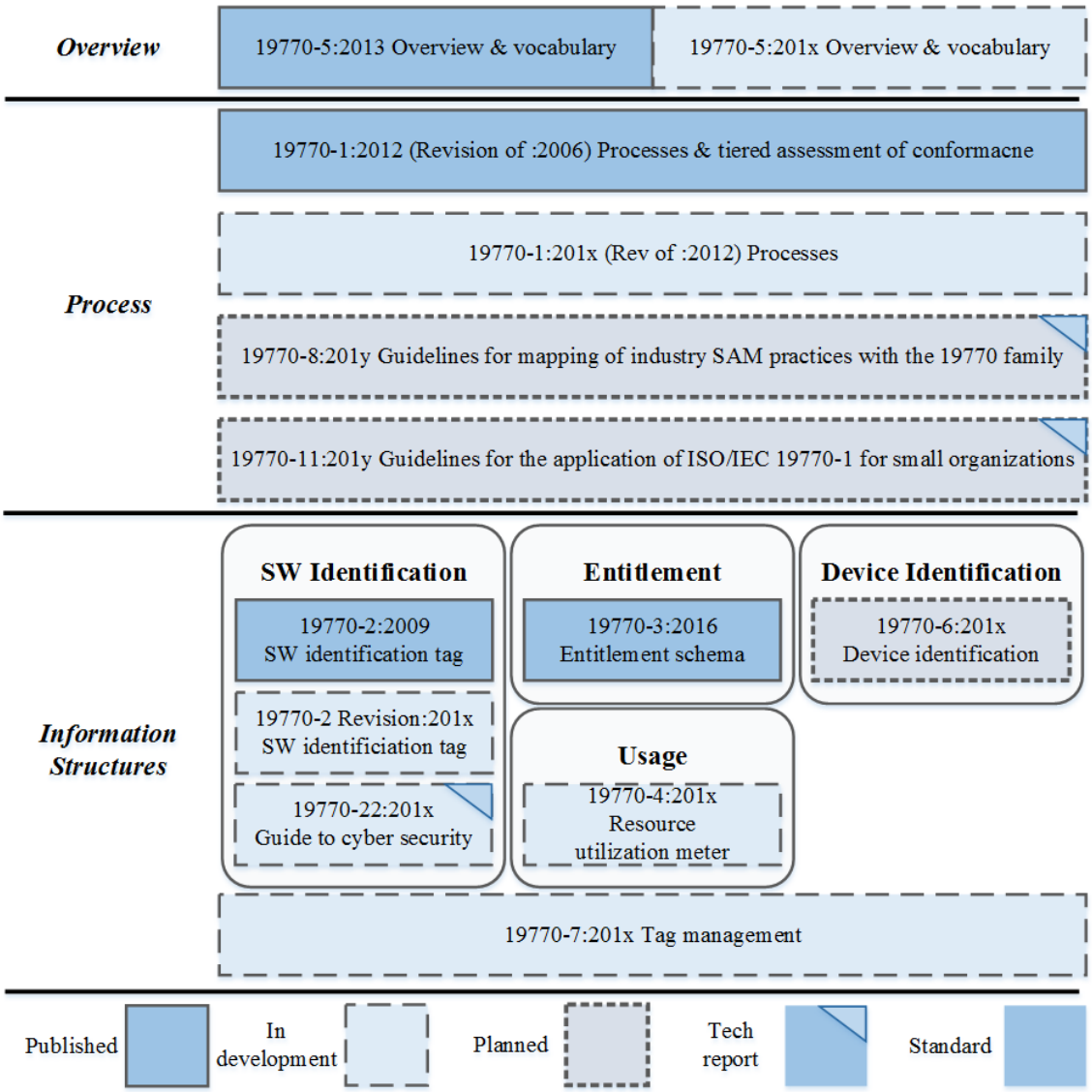


Figure 5. ISO/IEC 19770 family of standards categorized in purpose-based categories. (Restructured from ISO/IEC 19770-5 2015: 14.)

3.1 ISO/IEC 19770-1

ISO/IEC 19770-1, titled as "Information technology – Software asset management – Part 1: Processes and tiered assessment of conformance", is the first part of the family of ISO/IEC 19770 standards. As ISO/IEC 19770-2, also ISO/IEC 19770-1 is titled to be part of the set of SAM. Because of this, many of the descriptions of the standard are addressed for SAM, although later perceived to refer to the family of ITAM. ISO/IEC 19770-1:2012

is the second edition of the ISO/IEC 19770-1 standard, which replaces the first edition, ISO/IEC 19770-1:2006. The 2012 edition has received a technical revision compared to the previous edition (ISO/IEC 19770-1 2012: *iv*).

3.1.1 Coverage

The ISO/IEC 19770's first part applies to ITAM processes by the context of SAM. Although being the first part of a family of standards, ISO/IEC 19770-1 standard's implemental approach is intended to enable organizations to achieve immediate beneficial results. ISO/IEC 19770-1 is applicable for an organization of any size or field of business which can be labeled as a legal entity. Additionally, the SAM processes can be outsourced, yet still be recognized by the standardization. (ISO/IEC 19770-1 2012: 1.)

All software assets and all assets which are required to use or manage software assets belong to the scope of ISO/IEC 19770-1. The software definition covers both executables, such as applications and operating systems, and non-executables, which could be templates, documents and data in general. Software may appear in the form of use right, as a media including a copy of the software or as a use-ready software. Software-related assets, or in other words non-software assets, includes all hardware equipment which is required for software's usage or which can be further utilized with a software. ISO/IEC 19770-1 also lists properties of an asset relevant to the asset's management as part of the scope. This could be license users, owner relationships or the infrastructure of the IT amongst others. (ISO/IEC 19770-1 2012: 1–2.)

The standard's coverage is also limited in several aspects. The processes concerning SAM do not include detailing for methods or processes which are needed to meet the requirements of the standard. Not only is detailing excluded, but also the order of implementation steps is not defined. This concerns the total of SAM's implementation and the minor parts of it such as processes' sequencing. An exception for this is the general sequence of the

context, meaning that for example planning should be done before implementation. Another limitation to add is that the standard does not detail the level of documentation to be done. (ISO/IEC 19770-1 2012: 3.)

Organizations are allowed to narrow the scope of the certification by the definitions described in the certification's Clause-chapter. For example, organizations may target the asset management to specified manufacturers because of their higher priority. These scopes, reviewed to be unambiguous, should still answer to the desired objectives and the benefits available which as a total form the full conformance. (ISO/IEC 19770-1 2012: *v*, *vii* & 1.)

3.1.2 Tiers

Tiering is an efficient way to sequence the standard's accomplishment process. With a limited number of tiers can be provided simplicity and highlight the priorities of the stages within the standard. In ISO/IEC 19770-1 standard's case, the standard has been separated to four cumulative tiers because of the feedback received in the development phase. Organizations' wishes have been that the standard's part could be accomplished in increments. The tier-model allows the organizations to be recognized by their ability to publicly display that certification has been achieved to a stated tier in the form of free-standing independent certification. The tier model also corresponds to the natural progress of development in the standard's implementation which again reflects the proposed priority in management aspect. Although each tier could be certified separately, which would make it possible to try to achieve a tier of a higher number before the lower ones, the tiers have a strong relationship to the previous tier or tiers, and their performance highly depends on the quality of work done in the previous tier. (ISO/IEC 19770-1 2012: *v–vii* & 33.)

The first three tiers of SAM each reflect to a set of objects, whereas Tier 4 forms the total of the process areas and outcomes. To meet an object set, the tier comprises a process

allocated to accomplish the task (ISO/IEC 19770-1 2012: *vii* & 39–42). The four tiers of the SAM, as layered on Figure 6, are described as following.

Tier 1: Trustworthy Data drives for license compliance and the attainment of primary SAM records. To achieve the Tier 1 of SAM, it is required to know and understand the assets owned to further manage them. Tier 1 also covers the base for license compliance demonstrability so that organizations conforming to the requirements can always know their compliance status with licensing. Trustworthy data is supported by the standards ISO/IEC 19770-2 and ISO/IEC 19770-3. (ISO/IEC 19770-1 2012: *vi* & 34–35.)

Tier 2: Practical Management is characterized by commissioning processes for SAM records and turning the active processes into quick wins. To achieve the Tier 2, organizations need to have a management control environment in action. Along the control environment is delivered an ability to achieve immediate benefits from the data delivered by Tier 1. (ISO/IEC 19770-1 2012: *vi*, 34 & 36.)

Tier 3: Operational Integration introduces the core life cycle process and related processes for managing the related operations. Tier 3's status of SAM outcomes as improved efficiency and effectiveness. This means, that the practices learned from Tier 1 and Tier 2 are integrated to the operational processes. Integrating is also supported by the standards ISO/IEC 19770-2 and ISO/IEC 19770-3. (ISO/IEC 19770-1 2012: *vi*, 34 & 37.)

Tier 4: Full ISO/IEC SAM Conformance represents the status where the organization has achieved the best-in-class strategy for SAM. In Tier 4 are handled the advanced steps of the asset management, such as extended life cycle processes for service management. Also tying the practices into strategical planning is addressed. (ISO/IEC 19770-1 2012: *vii*, 34 & 38.)

Tiers in ISO/IEC 19770-1 also address typical management problems in organizations. Tier 1 secures the scenario where the amount of knowingly owned assets differs greatly from the amount of discovered assets. Tier 2 drives the management to a direction where the sudden arouse of risks and opportunities with assets can be handled. Tier 3 motivates

the sometimes significant implementation work with already delivered success from immediate benefits. Tier 4 is the last of the tiers for a purpose – to provide the long-term beneficial impact by the basis of the first three tiers, which cannot be illustrated before the smaller scopes of SAM. (ISO/IEC 19770-1 2012: *vi* & 34.)

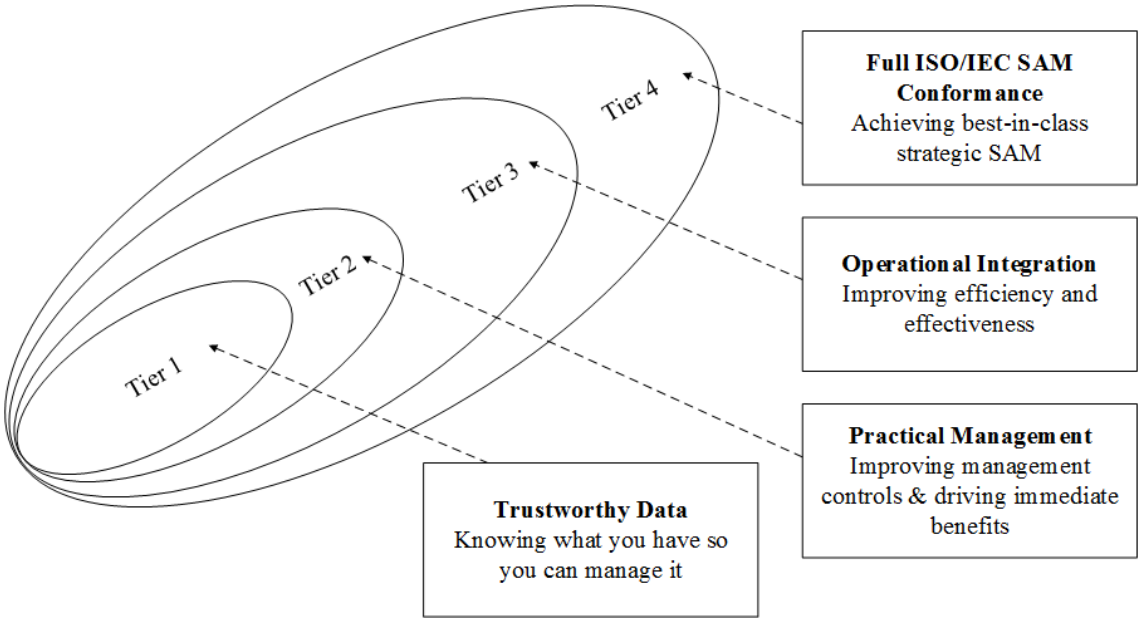


Figure 6. Software asset management in its four tiers. (ISO/IEC 19770-1 2012: *vi*.)

3.1.3 SAM Processes

When talking about software asset management, also control and protection of software assets and related assets are colligated into the concept besides management. Processes of SAM have been separated into three main categories: Organizational Management Processes for SAM, Core SAM Processes and Primary Process Interfaces for SAM. Each of the main categories hold several process areas inside them, as demonstrated on Table 2. (ISO/IEC 19770-1 2012: 6–7.)

Table 2. SAM processes in a framework-model consisting of three main process categories, in total six process groups and several process areas inside each process group. (ISO/IEC 19770-1 2012: 7.)

Organizational Management Processes for SAM			
Control Environment for SAM			
Corporate Governance Processes for SAM	Roles and Responsibilities for SAM	Policies, Processes and Procedures for SAM	Competence in SAM
Planning and Implementation Processes for SAM			
Planning for SAM	Implementation of SAM	Monitoring and Review of SAM	Continual Improvement of SAM
Core SAM Processes			
Inventory Processes for SAM			
Software Asset Identification	Software Asset Inventory Management	Software Asset Control	
Verification and Compliance Processes for SAM			
Software Asset Record Verification	Software Licensing Compliance	Software Asset Security Compliance	Conformance Verification for SAM
Operations Management Processes and Interfaces for SAM			
Relationship and Contract Management for SAM	Financial Management for SAM	Service Level Management for SAM	Security Management for SAM
Primary Process Interfaces for SAM			
Life Cycle Process Interfaces for SAM			
Change Management Process	Software Development Process	Software Deployment Process	Problem Management Process
Acquisition Process	Software Release Management Process	Incident Management Process	Retirement Process

In ISO/IEC 19770-1 SAM processes have been detailed in a level, where outcomes of the processes are designed to be immediately available for assessing. Outcomes however exclude the detailing of the action-steps to be taken in order to produce them. Several processes also have interfaces to another processes, which are reflected as interface activities. Interface activities are consequences when a process is executed, and another process needs to be invoked. As for example when an acquisition process is performed after a

purchase, a process to record the acquisition into an asset inventory needs to be invoked. (ISO/IEC 19770-1 2012: 7.)

Each process area is detailed in a full-length inside the standard, but in this work we focus on defining the general objectives and outcomes of each process group. Although SAM processes do not directly reflect to the tiers of the ISO/IEC 19770-1, which were explained in the previous chapter, there still are some applicabilities between the tiers and the objectives and outcomes of process groups (ISO/IEC 19770-1 2012: 6). The objectives, outcomes and applicable tiers of each process group of category Organizational Management Processes for SAM are described in Table 3, for category Core SAM Processes in Table 4 and for category Primary Process Interfaces for SAM in Table 5. In the following tables, when discussing about assets, or software and related assets, the definitions fall under the general definition of ITAM assets in the large picture. Additionally it is to be noted, that in the standard the outcomes are broken down into several subsections which detail and thus support the task of achieving the objects.

Table 3. The objectives, outcomes and applicable tiers of processes part of Organizational Management Processes for SAM. (ISO/IEC 19770-1 2012: 8–15.)

Main category	Process group	Objectives	Tiers	Outcomes
Organizational Management Processes for SAM	Control Environment for SAM	1. Internal recognition of responsibility	2, 4	Management system established and took into maintenance
		2. Roles and responsibilities for software and related assets are defined	2	
		3. SAM is maintained with clear policies, processes and procedures	2	
		4. Appropriate competence and expertise is available and applied in SAM	2, 4	
	Planning and Implementation Processes for SAM	1. Appropriately prepared and planned accomplishment for SAM objectives	2, 4	Effective and efficient SAM management in use
		2. Implementation of SAM objectives	4	
		3. Management objectives for SAM are achieved	2, 4	
		4. Improvement opportunities are discovered and acted upon when appropriate	4	

Table 4. The objectives, outcomes and applicable tiers of processes part of Core SAM Processes. (ISO/IEC 19770-1 2012: 16–26.)

Main category	Process group	Objectives	Tiers	Outcomes
Core SAM Processes	Inventory Processes for SAM	1. Assets have grouped classes and are defined by appropriate characteristics	1, 4	An inventory is created for software and related assets, the assets are recorded and taken into maintenance
		2. Physical instances of software assets are stored with characterizing properties	1, 4	
		3. Properties, status and approval information of software assets are controlled	4	
	Verification and Compliance Processes for SAM	4. Records are verified to be accurate and approved	1, 2, 4	Regularly performed verification and compliance of processes can detect exceptions to SAM policies and procedures
		5. Non-company owned assets are recorded and licensed	1	
		6. Software and related assets are used according to security requirements	3	
		7. SAM is under continuing compliance of ISO/IEC 19770-1	1, 2, 3, 4	
	Operations Management Processes and Interfaces for SAM	8. Relationships with SAM services or contracts providing organizations are managed	2, 3, 4	SAM is managed by operational management functions essential to overall SAM objectives
		9. Assets are budgeted and accounted, and information is readily available	2, 3	
		10. Levels of SAM related services are defined, recorded and managed	3	
		11. Information security management for SAM activities	4	

Table 5. The objectives, outcomes and applicable tiers of processes part of Organizational Management Processes for SAM. (ISO/IEC 19770-1 2012: 27–33.)

Main category	Process group	Objectives	Tiers	Outcomes
Primary Process Interfaces for SAM	Life Cycle Process Interfaces for SAM	1. All changes which impact on SAM are assesses, approved, implemented and reviewed	4	Life cycle processes (change management, acquisition, software development, software release management, software deployment, incident management, problem management and retirement) apply to SAM requirements set by ISO/IEC 19770-1
		2. Assets are controllably acquired and recorded	3	
		3. Software and related assets are developed in a way which considers SAM requirements	4	
		4. Release are planned and executed in a SAM supported way which considers changes	4	
		5. Software deployments and redeployments are executed according to SAM requirements	3	
		6. Incidents in ongoing operations related to assets are monitored and responded	4	
		7. Keep assets in operational condition through proactive identification and underlying problem addressing	4	
		8. Assets are removed from use or recycled according to company policy with a compliance to record-keeping requirements	3	

3.2 ISO/IEC 19770-2

ISO/IEC 19770-2, titled as “Information technology – Software asset management – Part 2: Software identification tag”, is the second part of the family of ISO/IEC 19770 standards. As ISO/IEC 19770-1, also ISO/IEC 19770-2 is titled to be part of the set of SAM. Because of this, many of the descriptions of the standard are addressed for SAM, although later perceived to refer to the family of ITAM. ISO/IEC 19770-2:2015 is the second edition of the ISO/IEC 19770-2 standard, which replaces the first edition, ISO/IEC 19770-2:2009. The 2015 edition has received a technical revision compared to the previous edition (ISO/IEC 19770-2 2015: *v*).

3.2.1 Software Identification Tag

Software identification (*SWID*) tag is a standardized data structure, which contains SWID information about a software product. These data structures are to support automated management functions in order to successfully store the SWID information (ISO/IEC 19770-2 2015: *vi*). A popular expression of SWID tag is in the form of an XML (*extensible markup language*)-file. SWID tags are created by the software’s producing party. In contrast, SWID tags are utilized by consumers, which may turn up to be tools or services used to extract the SWID information (ISO/IEC 19770-2 2015: 1). For a consumer, this information can be used for multiple purposes, such as license compliance, software security and logistical actions (ISO/IEC 19770-2 2015: *vi*).

For both producers and consumers of the software, detailed SWID information essentially provides price-efficient management assistance and automation possibilities. Security-wise SWID tags provide software management assisting data which may help to identify vulnerability identification and mitigation, or to help on identifying the software during an authentication. ISO/IEC 19770-2 has been developed to provide facilities especially for automating the IT processes, defined in the ISO/IEC 19770-1, for the purposes of security, compliance and logistics automation. Despite that ISO/IEC 19770-2 also provides information for human intelligibility for SWID, it is best to approach SWID tags as

an automated manner. Creating, managing and using SWID tags should be treated through a specialized or generalized tool. In addition to support the ISO/IEC 19770 family of standard's first part, ISO/IEC 19770-2 also cooperates with ISO/IEC 19770-3, an international standard for software entitlement schema. This part of ISO/IEC 19770 excludes the ITAM or related processes prescription necessary for reconciliation of software entitlements with SWID tags or other related requirements. Additionally excluded matters include product activation and launch controls. (ISO/IEC 19770-2 2015: *vi* & 1.)

As mentioned, the stakeholders of a software product can gain great advantage from the use of SWID tags through security and maintenance opportunities. The maintenance part covers software's creation, licensing, distribution, releasing, installation and continuous management. Through the use of SWID tags several benefits can be achieved in software maintenance, which most of them are listed below. (ISO/IEC 19770-2 2015: *vi*.)

- SWID tags offer metadata for consistent and authorized software identification
- Suites or groups of products can be identified and managed as a total
- Updates, issues or vulnerabilities can be related to installed software automatically
- Software information of software by different creators or for different platforms, toolsets or consumers can be facilitated for interoperability
- Enables automated license handling
- Products' information structure can be mapped for improved management
- Provides information structures about entities of producers and consumers
- Through digital signatures, enables the information's authentication and validity check
- Enables the SWID tagging for legacy software and for other already released software. (ISO/IEC 19770-2 2015: *vi–vii*.)

3.2.2 Conformance and Interoperability

In this chapter is described how SWID tags are created, what are the SWID tags' relationships and how the SWID information is used by consumers. SWID tags need to meet certain requirements to be in conformance with the standardization in order to be facilitated for the opportunities and advantages detailed in the previous chapter. Through the conformance of SWID tags can be created interoperability between tag producers and the tag consumers.

SWID tag is in conformance with ISO/IEC 19770-2 if the tag's data structure follows the restrictions set by the standard. For a consuming application, conformance with ISO/IEC 19770-2 comes from the sum of syntax and semantics. This means, that the tag consumer accepts all SWID tags in conformance; SWID information is processed in a consistent manner consistent with the semantic definitions of ISO/IEC 19770-2; and used XML schema definition (*XSD*) is identified and processes in consistence with the used version of XSD. For a platform to be in conformance with ISO/IEC 19770-2, the platform needs to provide an interface for adding, retrieving, enumerating and removing SWID information. Also the platform needs to support storing and retrieving of SWID tags from a file storage environment. ISO/IEC 19770-2 recommends the use of standardized data types in the form of XSD to enable an automatic validation provided by a consistent structure. (ISO/IEC 19770-2 2015: 3 & 10.)

SWID tags are usually created and maintained by the developer of the software. In cases when software does not have SWID tags, they are often created by a SWID tag discovery tool. The initial tag created by either of the cases becomes a primary SWID tag. SWID tags should only be modified by the original creators of the tags – the one named as the "tagCreator", which is detailed in the chapter 3.2.4. When the responsibility is unambiguously linked to the creator, it provides an authority for the data of a given tag. When additional information should be associated with a SWID tag by other than the tag's creator, this can be done by creating a supplemental SWID tag which refers to the SWID tag to be supplemented. (ISO/IEC 19770-2 2015: 3–4.)

As SWID tags define the data structure of a software product, it becomes a combination of many tags to form the total. Consequently the relationships between SWID tags are defined by using SWID links. SWID data structure may contain three different types of relationships: pre-installation data attribute, SWID patch attribute, and SWID supplemental attribute. (ISO/IEC 19770-2 2015: 4–5.)

Pre-installation data attribute fits for a scenario where a software under distribution is typically in a pre-installed structure and includes the program to setup the software. Consumer-wise the interest is in the software to be installed. SWID tags should therefore identify and detail the software also in its pre-installed form through pre-installation data attributes. (ISO/IEC 19770-2 2015: 4.)

SWID patch attributes are provided with software patches. A key detail for software patches is to indicate them being a patch by having the attribute "patch" set to be "true". Patch's SWID tags should also indicate the product the patch links to, and also the possible dependency patches. If a patch provides a cumulative update, the superseded patches need to be provided through tags as well. When none of the above tags are provided, it implies the patch can be installed independently. (ISO/IEC 19770-2 2015: 4–5.)

SWID supplemental attribute is, as suggested, linked to supplemental SWID tags. SWID supplemental attributes are directly associated to a software product's primary tag. When a primary SWID tag needs to be supplemented, the supplemental attributes need to be specified as "supplemental" with a value of "true". (ISO/IEC 19770-2 2015: 5.)

3.2.3 Implementation and Authenticity

SWID tag file is defined in an XML data structure format. ISO/IEC 19770-2 has a special definition for the XSD to be used. This is made to be publicly available at http://standards.iso.org/iso/19770/-2/2015-current/schema.xsd (ISO/IEC 19770-2 2015: 6 & 39–58). SWID tag is installed when a software licensor with a conformance to ISO/IEC 19770-2 provides the tag with the installation media of a software associating the tag, and

the actual software is installed. The same applies for uninstallations or when a software's release is changed (ISO/IEC 19770-2 2015: 6).

SWID tags should work in a platform independent manner, but there can be differences how a platform manages them. ISO/IEC 19770-2 lists two methods for platform-independent SWID tag accessing: SWID tag APIs (*application programming interface*); and SWID tag file storing along the installed application. SWID tag API method still requires a stored tag file when applicable, but it enables the use of operating system level service to control the management of the tag. By using the API, several additional information about the software usage can be stored, and a more effective and robust discovery process can be implemented. For a stored SWID tag file, tag data can still be processed by relying on a consistently similarly located swidtag-file accessing. (ISO/IEC 19770-2 2015: 11.)

Primarily SWID tag data is retrieved from a repository popularized by an XML-file through an API. In cases when an API is not available, the data should always be located in an XML-file at device's file system's subdirectory "swidtag". This directory is to be the same as the software component's installation location. If a file system is not available, the SWID tag data is to be stored in a location specified by the device's platform provider. This case allows an exception of using an alternative format besides XML when necessary. Additionally SWID tag data can be made accessible through a uniform resource identifier (*URI*). (ISO/IEC 19770-2 2015: 6–7.)

As SWID tags may be created by different parties, and the nature of SWID tags does not necessarily require a centralized registration of the tags, there has been introduced a unique registration ID (*regid*). Regid uses the form of URI to provide a unique naming authority identifier. By having a naming authority, the initial regid used by an organization becomes a consistently used identifier used for all software developed by the organization. (ISO/IEC 19770-2 2015: 7.)

Regid are suggested to use the http scheme with a minimum string required form. Therefore for example a URI "http://www.example.com" would be used as "example.com".

When an organization “example” would identify its software with the name “softwareProduct”, the regid could follow either a path-based form or a host-named form. Path-based regid form would therefore be “example.com/softwareproduct” whereas host-named form would be “softwareproduct.example.com”. (ISO/IEC 19770-2 2015: 7–8.)

Another identifying elements with SWID tags are tag identifiers and SWID tag file names. Tag identifiers are stored in the “tagId” value with a globally unique value. This is to be unique for every SWID tag by using a recommendation of a minimum 16 byte identifier. Unique SWID tag file names apply for installed SWID tags. SWID tags receives their definition from the XML-files and are stored with a .swidtag extension. The base filename, which excludes the extension, shall be globally unique for both the product and the tag creator. A recommendation by ISO/IEC 19770-2 is to use the naming convention of “<tag creator> + <product name>.swid”. (ISO/IEC 19770-2 2015: 8.)

Authenticity is used to validate that the discovered tag is not altered and that the tag provider is confirmed through the use of built-in digital signatures. Digital signatures are not a required feature for SWID tags. When signatures are used, they shall follow the World Wide Web Consortium’s recommendation which defines the XML syntax of the signature, and be enveloped with a stored timestamp validation. (ISO/IEC 19770-2 2015: 9.)

Elements of SWID tags, which are further detailed in the chapter 3.2.4, include “Payload” and “Evidence” elements, which may also be used to provide authenticity for a software product. Payload elements can be used to validate that the files in a directory are designed to be installed along the software item. Evidence elements can be used to collect software information when a SWID tag is not present with the software. The collected discovery data is sent to a server, compared and analyzed. An appropriately matching SWID tag is then created and sent to the client device to place the SWID tag along the software. (ISO/IEC 19770-2 2015: 10.)

3.2.4 Elements

ISO/IEC 19770-2 defines the data values and types to be used for SWID tags. These are specified in XML syntax suitable for SWID tag creation. Data values are elements of "SoftwareIdentity" element that, as suggested, include the information about the software component in question. These can be for example the name and the version of the software component. Data types are XML types which describe the structure and use case of a certain type. For example "Directory" and "File" are data types. (ISO/IEC 19770-2 2015: 12.)

ISO/IEC 19770-2 does not require a centralized tag management for validating the uniqueness of the tags created by a tag producer. Therefore it is only recommended for a tag producers to maintain a repository of all SWID tags created. This way the uniqueness of unique identifiers and normalization of recurring tag creator identifying elements can be validated. (ISO/IEC 19770-2 2015: 11–12.)

SWID tags may have a widely varying structure, which is why the minimum data values required for a SWID tag is a relatively limited set of information. Additionally some attributes have a default value, which is why they are also included in the default set of attributes. The attributes with a default value may assist on identifying the software product's version by setting the "version" to a default value of "0.0", unless otherwise specified. Besides the minimum requirements, there are also recommended SWID tag data values, which should be utilized whenever possible. An advantage of the recommended SWID tag data values in use is that by having them available, IT team's task to automate asset related processes can be made more complete. These minimum data requirements and recommended SWID tag data values are mentioned in Table 6 so that the table demonstrates all of the recommended SWID tag data items, their default values if specified, and a bolded text styling if the data item is part of the required SWID tag data values. (ISO/IEC 19770-2 2015: 12–13.)

Table 6. Recommended SWID tag data values and their default values if specified by ISO/IEC 19770-2. Data values with a bolded text styling indicate that the data values are required to be included in a SWID tag. (ISO/IEC 19770-2 2015: 12–13.)

Element name	**Attribute**		**Default value**
SoftwareIdentity		**name**	
		tagVersion	0
		tagId	
		version	0.0
		versionScheme	multipartnumeric
		patch	false
		supplemental	false
Entity	role	**TagCreator.role**	
	regid	**TagCreator.regid**	http://invalid.unavailable
	name	**TagCreator.name**	
Meta	product		

3.3 ISO/IEC 19770-3

The addressing of ISO/IEC 19770-3 is divided into three subchapters. The first subchapter, 3.3.1, defines an overview for ISO/IEC 19770-3; opportunities available through the standard; how the terminology is to be addressed when working with this standard and the ITAM guideline generated in this thesis; and the conformance specification of the standard. The interoperability of the schemas is detailed in the chapter 3.3.2, and implementation of entitlement schema processes including entitlement file description are detailed in the chapter 3.3.3.

3.3.1 Coverage

ISO/IEC 19770-3, titled as “Information technology – IT asset management – Part 3: Entitlement schema”, is the third part of the family of ISO/IEC 19770 standards. ISO/IEC 19770-3:2016 is the first edition of the ISO/IEC 19770-3 standard, meaning it has not received any revisions since its release. The standard addresses the software entitlement schema (also referred as *Ent*), a key part of software licenses, by providing a technical definition for the schema. What is excluded, are the processes and software identifying mechanisms linked to the software entitlements, as these have been defined in the parts 1 and 2 of the ISO/IEC 19770. In any conflicts with local policies, standards, laws or such, the conflict is to be resolved before implementing ISO/IEC 19770-3. (ISO/IEC 19770-3 2016: 1; ISO 2017c.)

ISO/IEC 19770-3 defines software entitlement schema as an “information structure containing a digital encapsulation of a licensing transaction and its associated entitlement information”. The technical definition of a software entitlement schema includes the definition for common terminology usable when discussing software entitlements, and a schema which can be used for effectively describing several entitlement subjects. Additionally the standard specifies a format for encapsulation of software entitlements. The software entitlement schema can summarize the primary points of software entitlements such as metrics, limitations and usage rights. By the information included in the entitlement schema, compliance with license rights and limitations can be ensured; license usage can be optimized; and costs can be controlled. Additional data can be provided along with the entitlement schema to completely store the terms and conditions of a license agreement. The complete data structure can finally be allowed to be automatically measured and processes, but this is not required from the creators of entitlement schemas. (ISO/IEC 19770-3 2016: *vi* & 1 & 3; ISO 2017c.)

ISO/IEC 19770-3 considers primarily two practical aspects in its design. These are “maximum possible usability with legacy entitlement information”, and “maximum possible alignment with ISO/IEC 19770-2”. The first of these principles means, that the entitle-

ment schema is designed to maximally utilize any existing or previously existed entitlement information. The standard points out, that this requirement must not interfere the operability with the continuous entitlement processes, and *vice versa*. The latter practical principle means, that the standard for entitlement schema shall be implemented with understanding and joint use along with the standard for software identification tags. (ISO/IEC 19770-3 2016: *vi*.)

This part of ISO/IEC 19770 is intended to offer benefits for all of the stakeholders part of the life cycle of a software and software entitlements. ISO/IEC 19770-3 lists several of the many benefits which can be expected with a successful acquisition of entitlement schemas. The benefits are targeted to result in cost optimization, a more effortless proof of ownership, improved license compliance management and, in a larger scope, an industry-normalized terminology for entitlements (ISO/IEC 19770-3 2016: 1). These selected benefits are listed below by grouping the expected benefits into three groups of involved parties**.**

Benefits to software licensors (entitlement schema providers):

- Consumer can instantly recognize the details of the usage rights
- Can provide software asset license measuring and reporting facilities for the customers
- Improved license compliance awareness for end-users
- Better licensor–consumer relationship through improved performance. (ISO/IEC 19770-3 2016: *vi–vii*.)

Benefits to tool providers and software suppliers including packagers and releasers:

- Uniformed data receipt from software licensors
- Entitlement information in uniformed data structure
- Support for automated software license alteration requirements
- More structured compliance management and reporting features
- Better integrability between SAM tools with uniformed entitlement data management. (ISO/IEC 19770-3 2016: *vii*.)

Benefits to end-users including IT support personnel, asset managers and software consumers:

- Uniformed data receipt from software licensors, tool providers and suppliers
- Entitlement information in uniformed data structure
- Support for automated software license alteration requirements
- Through the use of entitlement schemas, more structured reporting features
- Improved compliance for SAM and software licenses enabled by standardized and licensed suppliers utilizing ISO/IEC 19770-2 software identification tag practices
- Unified and thus more manageable entitlement schema usage regardless of the platform. (ISO/IEC 19770-3 2016: *vii*.)

ISO/IEC 19770-3 defines terms, definitions and abbreviated terms (ISO/IEC 19770-3 2016: 2–7) as does the other parts of the ISO/IEC 19770 family of standards. While the terminology provided by this part of ISO/IEC 19770 has an underlined role in the expected outputs available by the implementation of entitlement schemas, they are not reviewed in this thesis to avoid ambiguous definitions. Therefore it is recommended to rely on the original standard when defining the terminology of this part.

Organization's responsibility when implementing ISO/IEC 19770-3 is to specify the extent of applicability. The conformance to the standard may be either on organization- or product-level. Product level conformance requires that each software under licensing is provided with a related entitlement schema which is to be in comply with this standard. Each product in compliance shall additionally be clearly stated. Software vendors can demonstrate their compliance to products by demonstrating the ISO/IEC 19770-3 compliant entitlement schemas. Final clause for product conformance is offered for tools which produce or process entitlement schemas. The conformance of such tools can be achieved by demonstrating that the handled entitlement schemas meet all the mandatory requirements of ISO/IEC 19770-3. (ISO/IEC 19770-3 2016: 8.)

Organization-level conformance includes conformance for products associated with the organization. The structure of the organization is to be clearly stated along with the products included in the compliance when defining the scope to be on organizational-level. Software licensor's and entitlement schema tool provider's conformance can be achieved by a demonstration of conformance requirements with associated software. For an organization which acts as the consumer of the software, and is therefore part of the acquisition and/or usage of the software, can achieve the full conformance by demonstrating that each of the software within the organization's scope have an entitlement schema which meets the mandatory requirements of ISO/IEC 19770-3. (ISO/IEC 19770-3 2016: 8.)

3.3.2 Interoperability

By interoperability, when talking about entitlement schemas, is meant how entitlement schemas interconnect with each other and furthermore can provide general advantage between the parties involved with the creation and processing of entitlement data. The interoperability can be used for example to determine a current state of a particular object in the organizational environment. This is done by ITAM tools which combine the data of several entitlement schemas. (ISO/IEC 19770-3 2016: 9.)

Besides the two design-related specifications for entitlement schemas mentioned in the previous chapter, entitlement schemas have other standardized design rules which help with the interoperability. The first of these rules is that entitlement schemas should not be modifiable, after they have been created and taken into use. In case of an incomplete or incorrect entitlement schema, the entitlement schema can be fully replaced or supplemented with a supplemental entitlement schema. If a supplemental entitlement schema is issued, it is to be revoked. Another design rule is that entitlement schemas must have a transactional nature, meaning the schemas need to have cross-organizationally stored transaction information and only own organization scope when representing individual actions. The final design rule is, that the entitlement schema identifiers are to be unique within a relevant environmental scope. This however does not require authentication-locked identifier registration when compared to ISO/IEC 19770-2. The uniqueness comes

from a globally unique identifier each entitlement schema has called “entId”. (ISO/IEC 19770-3 2016: 9 & 16.)

Entitlement schemas have an “entType” value, which defines the use case of the schema in question. Based on “entType”, a schema can be either a primary or a non-primary schema referring to its role as a source of entitlement information. Typically a non-primary schema means that the schema is used to contain supplemental information (ISO/IEC 19770-3 2016: 13–14). There are five different types, which each of them is listed and detailed below in Table 7.

Table 7. entType values of entitlement schemas defined. (ISO/IEC 19770-3 2016: 14.)

entType	**Definition**
Initial	A primary entitlement schema type, which is usually created by a software licensor when an initial schema for a software is created.
Consolidation	A primary entitlement schema which consolidates other entitlement schemas. Consolidation-type entitlement schemas are usually created by the end-users for different reasons. Typically used to consolidate data and information of several entitlement schemas, but also information not yet included in any existing schema.
AllocationReceived	A primary entitlement schema, created when an entitlement is allocated from an entity to another. The ownership of the entitlement is still with the original entity.
TransferReceived	A primary entitlement schema which receives a legal transfer and thus an ownership change from an entity to another. This type is used to have a distinction between an Initial entType, as otherwise the transfer record might not always be indicated.
Supplemental	A non-primary entitlement schema entType used when the entitlement schema supplements a primary entitlement schema.

For entitlement schemas with the “entType” Supplemental there are detailed types specified by the value “supplementalEntType”. ISO/IEC 19770-3 provides six different types, but also allows the use of any else type-value which could be used for an unspecified use case (ISO/IEC 19770-3 2016: 14 & 16). These six types are listed and detailed below in Table 8.

Table 8. The six different supplementalEntType values defined. (ISO/IEC 19770-3 2016: 15–16.)

supplemental-EntType	**Definition**
InfoAdded	Used when a supplemental schema adds information to a primary entitlement schema.
Revocation	Used when a supplemental entitlement schema revokes another entitlement schema. A detail of which entitlement schema is revoked is left in the “linkedToPrimaryEntId”-attribute.
Condolidation-Part	Used when a supplemental entitlement schema’s primary entitlement schema is consolidated. In this case, as the primary entitlement schema as indicated by “linktedToPrimaryEntId” shall have a value “Consolidation”, the supplementary entitlement schema is considered as consolidated.
AllocationSent	A corresponding part to a primary entitlement schema with an entType “AllocationReceived”, which indicates an allocation from the current entity to another.
TransferSent	A corresponding part to a primary entitlement schema with an entType “TransferReceived”, which indicates a transfer from the current entity to another. “linkedToPrimaryEntId” shall refer to the source entitlement schema where the transfer is being made from.
Archived	Used when archiving an existing entitlement schema, which shall be linked to the supplemental entitlement schema. Archiving indicates, that the entitlement schema has been removed from use.

As mentioned above, entitlement schemas receive their uniqueness from “entId” identifiers. Additionally entitlement schemas have also three other globally unique identifiers, namely “regid”, “persistentId” and “linkContentId”. Regid follows the same definition as explained in the chapter 3.2.3, which means it uses a URI reference. Persistent software identification, shortened as “persistentId”, needs to be a globally unique identifier at least within its limited context such as the software licensor’s context. “persistentId” is used to identify each product installed regardless of their version. Both of the mentioned identifiers are recommended to use a 16 byte globally unique identifier, but when not possible, an identifier can be constructed by concatenating the software product’s details. ISO/IEC 19770-3 provides an example for this in the following way: *regid* + *productName* + *version* + *edition* + *revision* + ….. The third identifier, “linkContentId”, is used as an identifier for the download-source of terms and conditions. Besides the globally unique identifiers, there are several other properties within entitlement schemas which could be standardized to provide an all-round benefit for the involved parties. These properties include but are not limited to “role”, “limit” and “supplementalEntType”. (ISO/IEC 19770-3 2016: 16–18 & 27 & 32.)

3.3.3 Implementation

Entitlement schemas can be created by anyone, but the original primary entitlement schemas are preferably created by the software licensor. Entitlement schema created by a software licensor provides trustworthiness, but does not guarantee it. The final confidence shall always be laid upon the documentation of the contract, which includes the terms and conditions. Entitlement schemas’ trustworthiness can be defined by two qualities: authority and authentication. Authority comes from the creator of the software licensor, as this person or organization is expected to always have the highest authority and therefore highest trustworthiness when addressing the associated entitlement schema. Authentication means, that the entitlement schemas are expected to be digitally signed following the World Wide Web Consortium’s recommendation, and thus providing an authenticity. Through authority and authentication can be ensured that the entitlement schemas are not modified by anyone after the latest signer. (ISO/IEC 19770-3 2016: 18–19.)

ISO/IEC 19770-3 defines a file naming pattern for entitlement schemas. If entitlement schema is the only schema in a file, it should follow the pattern <*entCreatorRegid*>_<*product*>_<*entId*>.ent. When there are multiple entitlement schemas in a file, the pattern is changed slightly and should be in the form of <*entCreatorRegid*>_multi_<*entId*>.ent. "entCreatorRegid" is the value of regid for the entCreator Entity, and "entId" shall be the first entitlement schema in the file it is related with. (ISO/IEC 19770-3 2016: 19.)

Entitlement schemas are expected to be stored in a data structure of own choice by the organizations. This data structure could be for example a database or a spreadsheet. Generally the ISO/IEC 19770-3 refers to this storage as an "Ent library". Furthermore Ent library can be used for validating the uniqueness of identifiers, normalized element naming and for audit reasons, as entitlement schemas are meant to store external events and actions, and are not meant to act as action establishers. Optionally Ent library can also be used as a source for recovery for end-users. (ISO/IEC 19770-3 2016: 10 & 19–21.)

ISO/IEC 19770-3 demands on the flexibility when using and viewing entitlement schemas. The simplest approach would be to use a spreadsheet tool, but for full functionality a more advanced and targeted tool should be used. Yet, a spreadsheet tool should be capable of exporting entitlement information for further use. For managing entitlement schemas, a specialized tool is not only suggested but also expected. Such a tool is suggested for several reasons: A completely stored data structure may extend the capabilities of a simple spreadsheet tools in occurrence listing and detailing; majority of entitlement information is not normalized nor classified; properties with significantly large amount of text are expected; a consistent terminology for entitlement-context is expected; and entitlement information should be exportable for presenting and analyzing purposes. (ISO/IEC 19770-3 2016: 20.)

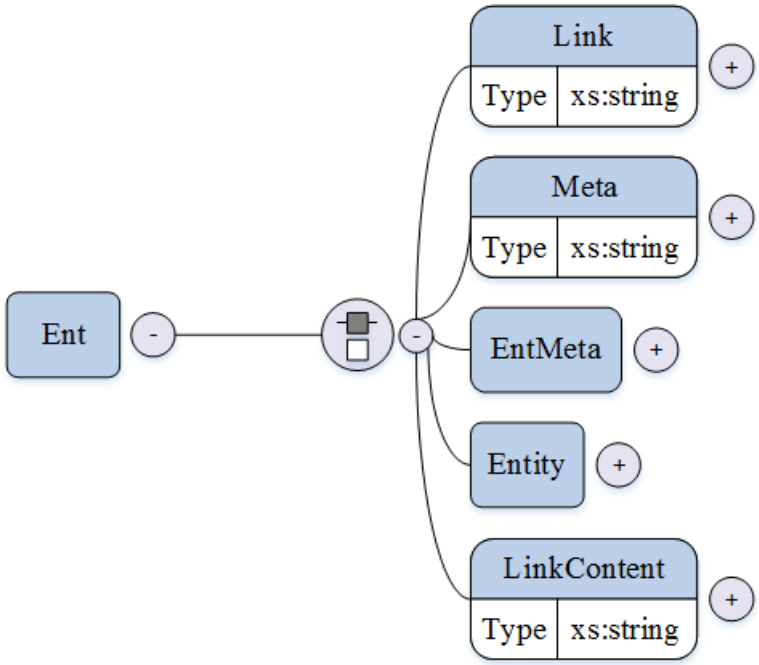
ISO/IEC 19770-3 defines a detail-level data specification for entitlement files. This includes standardized properties with normalized values, types and definitions for each in their suggested form – XML syntax. ISO/IEC 19770-3 and ISO/IEC 19770-2 are designed to align closely, which results in a possibility to use any of the specifications of

SWID elements or attributes in this part of the ISO/IEC 19770 too. (ISO/IEC 19770-3 2016: 21.)

Entitlement schemas have several use cases, which limits its design in set minimum requirements. ISO/IEC 19770-3 marks the minimum data requirements with a label "M1" in the definitions, meaning "mandatory in all Ents". The "M1" level is also significant as it is the only level to be flagged to be in conformance with ISO/IEC 19770 by default. The other requirement levels are "M2", "O1" and "O2", respectively meaning "mandatory in the context of the element", "optional but recommended" and "optional". To meet the minimum, the XML schema must have the following attributes defined: For Ent (Entitlement), <*entId*>, <*entCreationDate*>, and <*entType*>; and for Entity, "entCreator"-element's <*role*>, <*regid*>, and <*name*>. Specific use cases add more detail such as added mandatory attributes or more optionality in attributes. (ISO/IEC 19770-3 2016: 21 & 23.)

The structure of an entitlement schema is based on an element "Ent". A single file can include more than one "Ent" elements. "Ent" element shall include one or more "Entity" elements, which should detail the many roles of the entitlement schema. "Ent" element shall also include one or more "EntMeta" elements, which summarizes the key metadata of the entitlement information. Furthermore, "EntMeta" elements shall have one or more "Right" elements, which details the rights end-users receives from the software licensor. Besides these elements, there are several which may exist depending on the use case. (ISO/IEC 19770-3 2016: 22, 26 & 37.)

ISO/IEC 19770-3 provides examples for entitlement schemas (ISO/IEC 19770-3 2016: 55–61). Additionally the standard includes the Unified Modeling Language (*UML*) model of an entitlement schema and each level of elements in an XML syntax (ISO/IEC 19770-3 2016: 50–54). An example of this is illustrated in the Figure 7.

Diagram	
Children	**EntMeta**, **Entity**, **Link**, **LinkContent**, **Meta**

Source	`<xs:element name="Ent">`
	`  <xs:complexType mixed="true">`
	`  <xs:choice minOccurs="1" maxOccurs="unbounded">`
	`  <xs:element ref="Link"/>`
	`  <xs:element ref="Meta"/>`
	`  <xs:element ref="EntMeta"/>`
	`  <xs:element ref="Entity"/>`
	`  <xs:element ref="LinkContent"/>`
	`  </xs:choice>`
	`  </xs:complexType>`
	`</xs:element>`

Figure 7. ”Ent” element in its UML model and XML documentation form. (Restructured from ISO/IEC 19770-3 2016: 50.)

3.4 ISO/IEC 19770-4

3.4.1 Coverage

ISO/IEC 19770-4, titled as "Information technology – IT asset management – Part 4: Resource utilization measurement", is the fourth part of the family of ISO/IEC 19770 standards. In this thesis is used the DIS version of ISO/IEC 19770-4:2016 as the standard for resource utilization measurement was not released at the time the study was conducted making the full reference number to be used "ISO/IEC DIS 19770-4:2016". Since the standard has gone through the DIS ballot stage, it has progressed into the Approval-stage which is the last stage before the standard's publication (ISO 2016; ISO 2017d). Prior to ISO/IEC DIS 19770-4:2016 there are no previously published editions of ISO/IEC 19770-4. ISO/IEC 19770-4 is designed to co-operate with the other standards part of the ISO/IEC 19770 family of standards (ISO/IEC DIS 19770-4 2016: *vi*).

ISO/IEC 19770-4 is applicable for three different groups of IT asset stakeholders. These are a) software consumers and IT asset users, b) manufacturers of IT assets including software creators, and c) tool providers. The standard excludes the related ITAM processes for integrating resource utilization information with other information of IT assets, which may as for example be obtained through the implementation of ISO/IEC 19770-2 and ISO/IEC 19770-3. In any conflicts with local policies, standards, laws or such, the conflict is to be resolved before implementing ISO/IEC 19770-4. (ISO/IEC DIS 19770-4 2016: 1.)

ISO/IEC DIS 19770-4 lists specific expected key benefits for three different groups of stakeholders. These are introduced below.

For software consumers and IT asset users:

1. Resource utilization measurement data enhances the compliance of IT assets and optimizes the usage.

2. Resource utilization measurement data has a provider-independent, human-readable syntax which can further improve the visibility of resource utilization.
3. Authoritative and quantitative ITAM can be implemented as the result of utilizing ISO/IEC 19770-2, ISO/IEC 19770-3 and ISO/IEC 19770-4's resource utilization information.
4. ISO/IEC 19770-4 provides facilities for performing improved ITAM in conformance to environment-friendly strategies. (ISO/IEC DIS 19770-4 2016: *vi–vii*.)

For manufacturers of IT assets including software creators:

1. Centrally managed resource utilization information generating for consumers.
2. Support for third-party tools without further added functionality for an IT asset.
3. Facilities for IT assets' real-time tracking and alerting abilities.
4. Support for untraditional asset utilization measurement techniques. (ISO/IEC DIS 19770-4 2016: *vii*.)

For tool vendors:

1. Ability to control the measurements of multiple types and instances of IT assets.
2. Enhanced usage information aggregating.
3. Improved features for resource utilization tracking with minimized time delay. (ISO/IEC DIS 19770-4 2016: *vii*.)

Resource utilization measurements are in conformance with this standard, when the resource utilization measurement obeys the normative rules and requirements specified in ISO/IEC 19770-4. An application, such as an IT asset or an automation tool, is in conformance with ISO/IEC 19770-4 when it is able to produce resource utilization measurements which are in conformance with ISO/IEC 19770-4 as described above. An entity designed to process resource utilization measurements is in conformance when the entity does not reject any XML-formatted resource utilization measurement which is in conformance with the standard; when the entity processes resource utilization information in a manner which is consistent with the semantic definitions of ISO/IEC 19770-4; and when the entity is able to identify the version and process the information of an XSD document. (ISO/IEC DIS 19770-4 2016: 4–5.)

3.4.2 Definition and Implementation

Resource utilization measurement is a standardized data structure often in the format of an XML file. With resource utilization measurement data structure can be identified and provided usage information about the resources associated with IT assets' usage. With this design is intended to provide benefits for all of the stakeholders part of the IT assets' life cycle, which some of them are detailed in the chapter 3.4.1. Resource utilization measurement is designed to be widely applicable and thus on purpose it has a generalized structure intended to facilitate its management. Resource utilization measurements are created by automatized IT asset monitoring tools or by the assets themselves, and generally processed by specialized tools or manually by the consumer-party. (ISO/IEC DIS 19770-4 2016: *vi* & 4–6.)

Resource utilization measurement consists of two kind of information: the identifier to a particular IT asset's instance, and the actual resource utilization information contained in a measurement element. Resource utilization measurements identify the related IT assets through SWID tags when they are available, but alternatively referencing the asset by its unique identifier resided in the Asset-element is possible. The measurement is defined within one or many elements. Each of such elements are to contain the information capture timestamp, the timestamp for the start of utilization, the ending timestamp of the utilization, the measurement type, and one or many values. Each defined timestamp shall be encoded as specified in ISO 8601. The mandatory information can be complemented with optional information of each value or measurement. (ISO/IEC DIS 19770-4 2016: 5–7.)

Besides the mentioned design practices, there are several other to be included in the implementation of resource utilization measurements. As resource utilization measurements do not require a centralized registration authority, they use regid to have an identifier for unique naming authority. As with the other parts of ISO/IEC 19770, in ISO/IEC 19770-4 the related regid shall use the form of a URI with the same design recommendations. In an organization-scope, once initialized, regid should be used in any further scenario which involved the use of regid. Another design practice is related to the XML format expected

from a resource utilization measurement file. The XML data structure shall be based on the XSD defined in the ISO/IEC 19770-4, which is made to be publicly available at http://standards.iso.org/iso/19770/-4/, or by referencing to the initial version of the XSD from the standard's Annex A. (ISO/IEC DIS 19770-4 2016: 6–7.)

Resource utilization measurement files have also some suggested and mandatory design rules to be considered when implemented as listed below:

- The files should be readable at any time despite overlapping actions
- If an XML element is incomplete, any tool processing the file should ignore such elements
- The files should be named as <*SWIDtagfilename*>.<*logname*>.integer, when a SWID tag file is available with the linked IT asset
- The files should be named according to a structure which guarantees a globally unique name within the context of the file creator and the product associated. One such naming convention, as suggested by the ISO/IEC 19770-4, would be <*name of the resource utilization measurement creator*>+<*product name*>.<*instanceidentifier*>.<*logname*>.integer
- The file extension containing resource utilization measurement data must be .rum. For example, when there is a linked SWID tag file, the complete filename should be <*SWIDtagfilename*>.<*logname*>.integer.rum
- Resource utilization measurement files exceeding the maximum file size according to the defined value shall have its name appended with a numbered suffix, and the data storing can be continued on a new file
- Resource utilization measurement files must not be automatically deleted when an associated asset becomes uninstalled or upgraded
- Resource utilization information must be manually extractable, and further managed and manipulated in a spreadsheet format.

The standard yields some choices of own will for the users for example with the resource utilization measurement file locating policies, the frequency of resource utilization measurement file generation, the use of digital signatures, and the use of XML nesting. (ISO/IEC DIS 19770-4 2016: 7–9.)

3.4.3 Schemas

A general resource utilization measurement item consists of linked data elements, which can be projected in the form of a schema. ISO/IEC 19770-4 defines a minimum resource utilization measurement data required for a schema's structure, which consists of the following elements:

- ResourceUtilization
- AssetIdentification, with one of the following child elements
    - Link, if the SWID tag exists
    - Asset, if the SWID tag does not exist
- Measurement, which shall hold at least the following attributes
    - logTime
    - metricName
    - startTime
    - endTime
- Value. (ISO/IEC DIS 19770-4 2016: 10.)

Additionally the standard defines a naming policy for the related elements and attributes to enable interoperability with SWID tags. Elements and attributes shall be consistently named with the associated XML counterparts. Of these, XML elements store XML attributes whereas XML attributes store the data. These can be identified by for example the naming rule of the items, as elements shall be named with a capital starting letter (AnExample), and attributes with a lower case starting letter (anExample) (ISO/IEC DIS 19770-4 2016: 11). It should be noted, that this naming rule is consistent thoroughly in the ISO/IEC 19770 family of standards.

ISO/IEC 19770-4 documents the data values of each of the schema's items with a detail of description of each item, and type, definition and optionality of each attribute and element. Each data value is also provided an XML-formatted example. Here we name each data value and its description as presented in the standard:

- "ResourceUtilization" element represents the root of the of the schema;
- "AssetIdentification" represents parent for child elements to identify the related asset;
- "Measurement" represents the measurement information related to the asset;
- "Value" represents the quantities the measurement;
- "Link" represents a data reference to another item, such as to a SWID tag;
- "Meta" represents an unlimited collection of related data;
- "Asset" represents a unique identifier to the related asset when a SWID tag is not available; and
- "Instance" represents an identifier of an asset's instance when it is necessary to distinguish an asset from multiple instances. (ISO/IEC DIS 19770-4 2016: 11–17.)

3.5 ISO/IEC 19770-5

ISO/IEC 19770-5, titled as "Information technology – IT asset management – Part 5: Overview and vocabulary", is the fifth part of the family of ISO/IEC 19770 standards. ISO/IEC 19770-5:2015 is the second edition of the ISO/IEC 19770-5 standard, which replaces the first edition, ISO/IEC 19770-5:2013. The 2015 edition has received a technical revision compared to the previous edition. Of the five standards of ISO/IEC 19770 family of standards, ISO/IEC 19770-5 presents the fundamental definition and terminology for the whole standard family, but also reasons why software asset and related IT assets should be managed in the first place. The overview-part of the ISO/IEC 19770-5 has been already detailed in the chapter 3 for sequencing reasons. (ISO/IEC 19770-5 2015: *iv–v.*)

The terminology provided by ISO/IEC 19770-5 includes several key terms which are present either thoroughly in the family of the standards, or are essential for a main chapter of the coverage. Below in Table 9 has been listed a selected set of terms and their summarized definition respectively.

Table 9. A selected set of terms and definitions of ISO/IEC 19770. (ISO/IEC 19770-5 2015: 1–6.)

Term	Definition
asset	An item, a thing or an entity which has potential or real value to its owner.
asset management	An activity to recognize and to put into action the value of an asset.
configuration item	An item under control of configuration management.
configuration management database	A database to contain all recorded details of configuration items.
element	Component part of an information structure to provide information about the related entity.
globally unique identifier	A generated 16-byte string of characters.
information structure	A structure that provides any kind of information relevant for managing a software asset.
process	A total of multiple activities which either interact with or relate to each other.
registration identifier	Also known as regid, entity's unique identifier.
software	Programs and any related procedures, rules and documentation of information technology environment.
software entitlement	License use rights for software agreed between the licensor and the consumer
software identification tag	SWID tag is an information structure which holds the identification information of a configuration item

Besides the ones mentioned in the Table 9, ISO/IEC 19770-5 provides additional definition for two more terms, namely *IT asset management* and *software asset management*. Asset management, "an activity to recognize and to put into action the value of an asset", holds the parent discipline of the two subsidiary discipline. An essential feature of asset management is the attempt to maximize the utilization and performance of an asset and thus as an output receive the highest available value while in comply with minimized costs and risks. The scope of asset management can be projected over the asset's life cycle as each part of the asset's life cycle has associations to asset management. The versatile data available through asset management's records can also provide primarily monitored key performance indicators. (ISO/IEC 19770-5 2015: 8.)

ITAM, as defined by ISO/IEC 19770-5, is about the asset management practices having IT assets and related infrastructure as the objects. Specific cases which fall beyond ITAM are for example the portability handling of portable IT assets, such as laptops. Software asset management focuses on all items which fall beyond the definition of a software with relevant life cycle management activities. Software asset management's special cases would include for example handling of distributed and virtually hosted assets. An important detail to note is that software asset management is defined as a "further sub-discipline" of asset management and "sub-discipline of ITAM" whereas ITAM would be a "sub-discipline" of asset management. Despite this, the scope of the both subsidiary disciplines have the same scope for practical reasons. (ISO/IEC 19770-5 2015: 8–9.)

Software assets are an increasingly complex, but also increasingly important group of manageable assets. The number of managed software assets has every reason to increase also in the future, which is why it is important for an organization to gain the best possible value from such assets. ISO/IEC 19770 family of standards provides practices, processes, guidance and regulations which can assist an organization in its overall software asset management and related IT asset management. This includes improved security, facilitated automatization for IT functionalities and data interoperability. ISO/IEC 19770-5 separates the available benefits into three subclauses: direct benefits; cost control; and risk management and mitigation. Some of the benefits listed by ISO/IEC 19770-5's have

been mentioned earlier, but the following listing shall bundle the benefits together. (ISO/IEC 19770-5: *v* & 9.)

The direct benefits through introducing and executing ITAM and therefore also software asset management include the following:

- An appropriate and efficient way to deploy software to the organization's members who can focus on fulfilling the set business objectives;
- an all-in-one information storage for transparent and effective decision making;
- improved speed and reliability on initializing new IT functionalities;
- a single point of source for end users to obtain equally available IT tools;
- IT can flexibly enable the technological requirements for new business requirements; and
- overall improved inner motivation and outer satisfaction through the IT provider's stabilized and improved performance resulting in less problems. (ISO/IEC 19770-5 2015: 9.)

Benefits in cost control can also be facilitated through the introduction of the many ITAM's parts. These benefits include the following:

- Reduced acquisition price with centralized purchase channels;
- by redeploying software licenses unnecessary purchases can be avoided;
- more efficient purchase process with a partner through information availability;
- by planning the ITAM processes, the inevitable asset management costs can be reduced with a multipurpose infrastructure;
- reduced support costs; and
- finding and analyzing the high cost points of the infrastructure. (ISO/IEC 19770-5 2015: 10.)

The organization's management and mitigation of risks can also receive several benefits through ITAM. This subclause of different to three further areas: operational management and mitigation of risks, security management and mitigation of risks, and compliance management and mitigation of risks. These benefits include the following:

- Operational management and mitigation for risks:
  - Decreased risk of IT service interruptions; and
  - decreased variation and risk of decrease of in quality in IT services.
- Security management and mitigation for risks:
  - Increased assurance for IT tools' author-proofing;
  - recognition of non-authorized software; and
  - transparency and auditability for software's patch processes and statuses.
- Compliance management and mitigation for risks:
  - Identifying information vulnerabilities, legal holes and other privacy concerns;
  - license management and auditing;
  - policy management and auditing; and
  - general prevention of harm which could damage the public image. (ISO/IEC 19770-5 2015: 10.)

ITAM and software asset management can be achieved through a variety of ways and by organizations of different sizes. The scope of included assets is broad, but ideally the implementation can use different delivery models or a mix of them, which could end up to be a mix of mobile functionalities and cloud-based mechanisms, as an example. Additionally the implementation steps are left to be undefined by the standard allowing flexibility for the IT practitioners pursuing for ITAM. ISO/IEC 19770 integrates to other related ISO and ISO/IEC standards which can ease the initialization of ISO/IEC 19770's implementation. These standards include ISO 9001, ISO/IEC 20000, ISO/IEC 27000 and ISO 55000. (ISO/IEC 19770-5 2015: 11–13.)

The evaluation of the outcomes of ITAM can be done for a partial conformance, or for full conformance. Partial conformance can be demonstrated by using the outcomes as the evidence, or alternatively by demonstrating that each processes objectives have been achieved. Full conformance at first requires that each tier's conformance meets the objectives through a demonstration as described above, but there are also two other requirements for a full conformance. One is to assess cross-tier process outcomes, and the second is to provide a documentation for any uncomplete objective which should demonstrate a consideration of the missing outcome and why it should not affect the acceptance with the objective in question. Furthermore the critical success factors of the asset management program underline the priority points and the expected outcomes. These are an expected ability to indicate the direction and ownership of the program presented by the executive management level; a clear definition of the program's scope, responsibilities and roles; and a demonstrable understanding of software use rights such as licenses and how they apply for the managed software assets. (ISO/IEC 19770-5 2015: 12–13.)

3.6 ISO/IEC 19770 Family's Other Parts

ISO/IEC 19770 family of standards consists of other standards excluded from detailing in this thesis. These are ISO/IEC 19770-6, ISO/IEC 19770-7, ISO/IEC 19770-8, ISO/IEC 19770-11 and ISO/IEC 19770-22. The statuses of these standards are varying, but none of them has received a draft version by the time the study was conducted. The statuses vary from a planned to the different parts of being under development, as indicated in the Table 1 presented in the chapter 3. Of these standards, ISO/IEC 19770-6, ISO/IEC 19770-7 and ISO/IEC 19770-22 provide information structure specifying content whereas ISO/IEC 19770-8 and ISO/IEC 19770-11 are technical reports by their type, which shall provide guidance for process standards (ISO/IEC 19770-5 2015: 15–18).

ISO/IEC 19770-6 details how to identify and manage devices with embedded software through the use of similar information structures as other standards in the family use. ISO/IEC 19770-7 defines a baseline for tag management for tags used in the family of standards. The baseline comes in the form of a roadmap and a guidance. ISO/IEC 19770-

22 addresses how the information structures defined by other standards in the family could be used with cyber security practices. The standard has a strong association with the standard ISO/IEC 19770-2 by defining how software tags could be used to pursue information security. (ISO/IEC 19770-5 2015: 17.)

ISO/IEC 19770-8's scope is on identifying the differences and correspondences of the definitions from existing industry and the ones used thoroughly in the ISO/IEC 19770 family. ISO/IEC 19770-8 is expected to provide more industry-related approaches for organizations looking to eventually have a full conformance to the family of standards. ISO/IEC 19770-11 provides a specific guidance for small organization on how to apply the processes of ISO/IEC 19770. The appliance obeys the tier-model of ISO/IEC 19770-1 and details an overall simplified model suitable also manual procedures by a limited group of people. (ISO/IEC 19770-5 2015: 15–16.)

4 CASE STUDY'S PLANNING

The study's theoretical part included the research on the related theory consisting of asset management and its subfields in the form of a literature review. The outcome from this was used to form an overall view of asset management's scope, key definitions, and to define enterprise asset management and ITAM. The related family of standards, ISO/IEC 19770, was defined and detailed with a focus on the family's parts 1–5. After the theoretical specification, an applicable research method, *action research*, was reviewed, and the parts suitable to be used for implementing a plan for ITAM for the target company were determined. Before moving to developing the plan, the current state analysis for the target company was done to fully understand the context the ITAM would be implemented upon.

4.1 Research Method

Although the topic of this study does not necessarily require a research method to be utilized in the background of the plan's development process, one was used, but only where it was applicable. The research method, action research, shall therefore be used in a way which excludes steps, processes and formality where perceived as unnecessary, while retaining the parts which can enhance the attainment of the study's objectives. Here we define action research's key concept and which of its content was found to be applicable for the study in question.

Kananen (2013) segregates two close terms, action research and design research, which may regionally have slightly different definitions. In Finland's context, action research and design research have a difference, which commonly cannot be taken as a self-evident fact. Action research differentiates primarily on the role of the researcher, as in action research the researcher participates in the development process, which would not be the case with design research. (Kananen 2013: 41.)

Action research has several subcategories, which many of them have a close connection to social sciences. The subcategories include “participatory research”, “critical action research”, “classroom action research”, “action learning”, “action science”, “soft systems approaches” and “industrial action research”. Of these subcategories, we have selected some of the ways of putting action research into practice from the subcategories “soft systems approaches” and “industrial action research”. (Kemmis & McTaggart 2005: 560–562.)

Soft systems approaches are an opposite of hard systems. In hard systems approaches a clear goal and a way-to-go would be identified and less communication is needed. Soft systems approaches aim to generate a solution for a set of problems with a possible change for management practices. Soft systems approaches are suitable for complex task solving, where the end result can be reached in several ways. This is done by the help of a researcher whose role is to work as a consultant in the process, and which may or may not be an external to the organization. The researcher shall work with the organization’s participants to formulate models of the current situation and to analyze them. Based on the models are created revised versions of the models as suggestions for improved workflows. (Checkland 2000: 14 & 54; Kemmis & McTaggart 2005: 562.)

Industrial action research has the similarity to soft systems approaches that it is also a consultant-driven process. Industrial action research is characterized as a collaboration which involves members from the different levels of an organization, and usually results in substantial changes on organizational and social cultures. The process of the knowledge gain could be a more formal operation, but the definition of the research type also allows more informal, crafted way of working which allows the organization to bring their own preferences to the conduct. (Kemmis & McTaggart 2005: 562.)

From the two subcategories of action research can be formed a research model we can use in this thesis. Soft systems approaches’ way of producing a revision in a less formal model in terms of avoiding problem-to-solution implementation can be used in this research. Industrial action research’s way of involving people of different levels of the organization also supports the research, as providing changes to organizational and social

aspects likewise does. The way of modeling the problem that shall be lead to an improved situation through analyzing by a multitude is visualized in the Figure 8.

The initial goal is to provide an improved coverage of assets, a unified way of handling assets, added internal communication and long-term cost efficiency – a mixture of short- and long-term benefits. The research starts with the extracting of the information of at least management and senior level about the organization's current ITAM and related practices using their own terms, the overview of the ITIL hierarchy and the expectations about improvements. The information can be gathered by interviewing, through a collaboration in work-context and by reading existing documentation (Stringer 1999: 67). With the available knowledge baseline, an improved model for ITAM can be proposed for the organization. This model shall be based on the information provided by the organization, and the best practices provided by the ITAM's theory and ISO/IEC 19770.

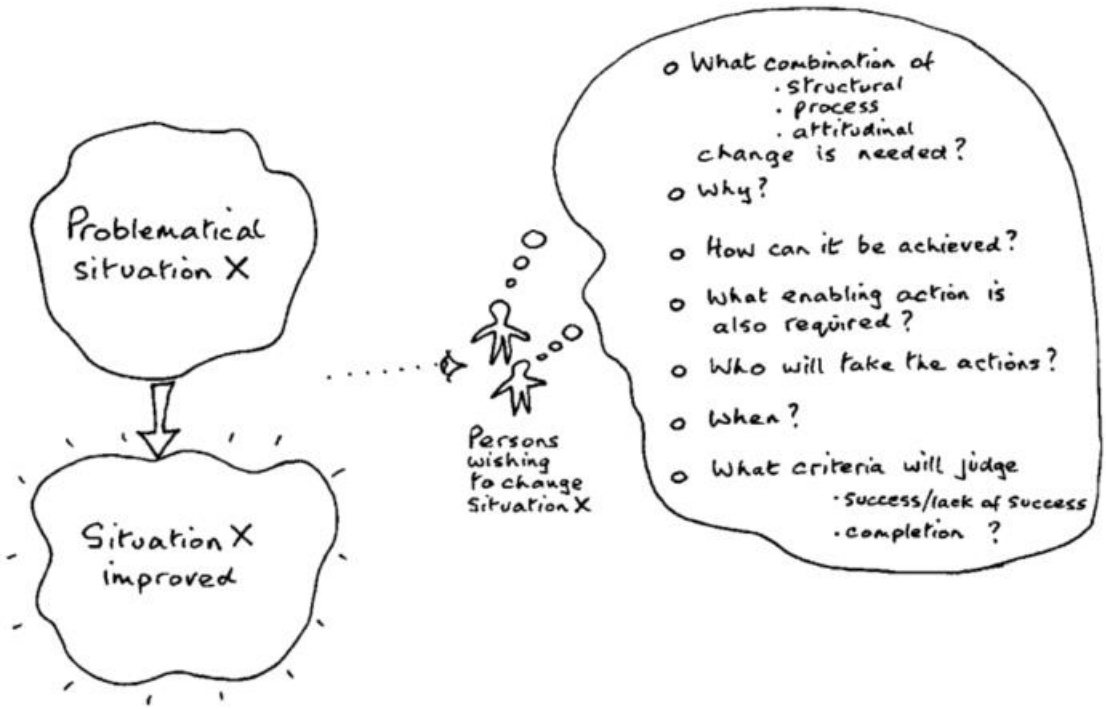


Figure 8. Analytical thinking by participants in an action research can address the problem thoroughly and find the ways how a problematical situation should be improved. (Checkland 2000: 34.)

Some remarks about the process should be made. By utilizing action research, we can ensure the social aspect and collaboration's input in the result. What separates consulting and action research is that the research can provide enhancements to all levels of the business by providing a distinguishable change to the activities of the organization's members (Kananen 2013: 40–41). Despite the mentioned informality in the used techniques, an action research uses the default stages of the research, namely planning, action, evaluation and follow-up, which each of them shall also be covered in this thesis (Stringer 1999 43–44; Kemmis & McTaggart 2005: 563–564; Kananen 2013: 42). The process of information gathering and implementation by involving the organization's management level (or, in other terms *stakeholders*) is suggested by both Finnish context of conducting an action research in information systems strategy (Reponen 1992: 1) and by the universal definition of action research considering the role of the researcher in the study (Stringer 1999: 25–26). Finally, an action research may be assumed as failed, if it does not result in a change or a difference within the organization the participants represent (Stringer 1999: 19).

4.2 Current State Analysis

The current state analysis is done for the company involved in the study, Wapice Ltd., by collecting information about the aforementioned subjects of ITIL and ITAM using action research's selected actions. The information will be based on the prior knowledge of the researcher and the colleagues representing the target company about the company's assets, asset management, used processes, used technologies and available asset storages. In addition the known deficiencies in the asset related processes are investigated.

Prior to the study, the process of an IT asset acquisition has been such that each acquisition has gone through an approval process which is stored as a ticket to the internal systems. Acquired IT assets, which are either connectable directly to the network, such as laptops, or indirectly through another asset, such as keyboards, are recorded automatically. Relevant details of an asset are included in the data collection. These include for example the asset's manufacturer; the asset's model; the latest timestamp of a connection;

and the primary user of the asset. The data is collected in timed cycles incrementally so that new assets are added when discovered and old records are updated if needed, and the data is being stored into an internal CMDB. If an asset receives updates, such as an updated component to a computer, the addition shall be acquired through the acquisition process, but the component becomes recorded as part of the computer it becomes attached to. Software assets are handled a bit differently than physically existing IT assets, as they have for example the installation date, version and possible license related information attached to them. Because of the large number of software in total, they are also handled in a separate database table or tables than other IT assets. License information of software are stored in a database table external to CMDB.

When an asset becomes deprecated, is replaced, or is taken out of use, the asset does not receive manual handling unless the asset has privacy confident attachments such as solid-state drives which shall receive a special handling. Instead, the asset becomes outdated in the context of the CMDB, as the latest synchronized timestamps start to go beyond the set limitation of active assets. With software, a similar dating is applied. Because of the dating, an old and a new version of an installed software may exist in the CMDB temporarily. Further history for software is additionally available.

Tag information of software exists only when the initial publisher, author or vendor has attached the information with the software. Besides tag information, the same applies for entitlement schemas and related entitlement information. Generally no information is supplemented among the IT assets. If an exception to this is done, the supplementing has not followed the ISO/IEC 19770 guidance on supplementing additional information prior to the study. Tag information, entitlement schemas or resource utilization measurement files have not been recorded centrally prior to this study.

The processes of ITAM are tied to the company's ITIL. This means, that ITAM supports the several managing related services of ITL, but also *vice versa*. The currently managed CMDB includes a database table for laptops and the components of each, consisting of around 1000 records. Another notable database table is for the software, where the records are at around 100,000. The total number of manageable assets therefore reaches to a five-

digit level. This suggests that many of the assets shall be treated through automated processes, but the most important or the most complex assets may have a treatment which involves manual handling. Generally the coverage of the assets is supposedly broad and comprehensive.

The known difficulties with the current approach for asset management are in the acquisition and decommission of the assets. Although both phases of the asset's life cycle have a current practice, they include challenges with the marking of the asset's status. The status of an asset when it is being stored during the middle of its life cycle is also something which has a vague definition, and should be defined more precisely.

The target company's initial asset management may have its biggest opportunities for improvement in the acquisition and decommissioning of assets, in the communication between the stakeholders of the asset throughout the life cycle, and in the commissioning of ISO/IEC 19770-1 practices thoroughly in order to facilitate the ITAM for further applicability of the ISO/IEC 19770 family of standards. As no tag nor entitlement schema related processes are performed in the target company, initializing ISO/IEC 19770-2's and ISO/IEC 19770-3's practices would be expected to be a significant addition to the current management practices with IT assets. With resource utilization measurement, the target company may be able to expand the current practices with a more tolerable amount of effort to have them at the ISO/IEC 19770-4's level.

5 DEVELOPMENT OF IT ASSET MANAGEMENT GUIDELINE

This chapter is divided into five parts, namely Description of the Guideline's Parts, Common Scenario Analysis, Proposed Implementation, Benefits and Liabilities, and Post-implementation. In the first subchapter we describe the content of the guideline to be proposed, and why the guideline is required. In the second subchapter an average scenario of an organization's ITAM is determined based on an existing literature and ISO/IEC 19770. In the third subchapter the actual proposal for the implementation is given. This chapter composes the core of the guideline provided for the target company. In the fourth subchapter the proposed guideline is evaluated with the aspects of how it can benefit the target company, but also by taking into account what liabilities the guideline yields. Finally in the fifth subchapter we define the post-implementation steps and tasks which should be taken into account after implementing the content of the guideline. These steps and tasks may be considered as optional duties, which can enhance the overall result obtainable through ITAM.

5.1 Description of the Guideline's Parts

Ultimately managing IT assets does not largely differ from managing any other assets besides the terminology. Compared to some assets from for example manufacturing industry, the lifespan of an IT asset may also be shorter, and IT assets may often exist only to provide a service for further use, but these do not change the way we do the management of the assets (Helstrom & Green 2011: 352). It shall also be kept in mind, that IT assets are both physical and non-physical assets. It becomes impossible to execute ITAM with software assets without considering their licenses, and without considering the hardware we use to run the software. ISO/IEC 19770 acknowledges this by having conformed to managing the many instances of IT assets starting by the ISO/IEC 19770-1 standard (ISO/IEC 19770-1 2012: *v*).

The Institute of Asset Management, IAM, states that "organisations should have guidance in place to support consistent development, evaluation and comparison of investment proposals" (IAM 2015: 44). Deriving from this purpose, we want to have a guideline for the IT assets' asset management to support the organization's continuous performance in several aspects. The guideline shall cover a strategical thinking for asset management corresponding with the planning-phase of the asset management process. The following concepts are considered within the guideline: consistency, risk tolerability, life cycle approach, asset management framework, needs of the stakeholders, assets' performance, asset management's adaptability, and continuous improvement (IAM 2015: 40). Most importantly of the mentioned, an answer to the needs of the stakeholders should be delivered, which should directly answer to the definitive demand of the target company.

The guideline receives its core structure from the life cycle model as visualized in the Figure 1 in the chapter 2.1. An additional effort will be done for defining the acquisition and decommission of an IT asset. We define the desired workflow of both of these phases with a step-by-step model. The demand of the target company is mixed with the ISO/IEC 19770 level of requirements which may equate to the full recognition for standardization, or provide partial conformance to the relevant standard. The guideline sets a related standard from ISO/IEC 19770 family of standards as a target when appropriate, meaning achieving the standardization comes after target company's need and demand when referring to the priorities.

The proposed implementation is structured in a chronological order. The plan consists of several concepts detailed earlier in this study. The concepts of the study are ITAM processes, SAM processes, tiers, standards of the ISO/IEC 19770, tools and authorities. These concepts are tied together with associations, sequences, responsibilities and categorizing connections.

5.2 Common Scenario Analysis

When an organization has challenges with some aspect of the asset management, it is commonly shared with other organizations with mutual features. Here we define some of the supposed weaknesses which a generic organization might have with asset management. These are added and partly counterpointed with expected findings of the ITAM's implementation. Therefore the defined items here are not limited to expected challenges, but also expected positive results are shared.

When moving into the implementation of the ISO/IEC 19770 driven ITAM practices, the order of development and minimum requirements might differ in a real-life scenario from the given model. This is expected and only means that the organization takes into account organization-specific exceptions, and existing processes and policies which need to be considered already in an early phase of the development (ISO/IEC 19770-1 2012: 34). The first remark that an organization is expected to discover when initializing a comprehensive asset management, is that there tends to be a significant difference in the expected amount of found assets when compared to the actually found amount of assets through the IT asset management's processes (ISO/IEC 19770-1 2012: 34). Bonham (2004: 145) suggests that this is often caused by the lack of recommissioning IT assets properly.

An asset management system commonly receives a clear definition of the responsibilities and roles within the system when the system becomes management-owned and inspected. Additionally this sets a mark of the expected first revision leading to the first improvements for the system. Found challenges within the system are often addressed to a group or a person to become solved. These challenges are usually to turn into quick results and rewards from the asset management. (ISO/IEC 19770-1 2012: 34.)

ISO/IEC 19770-1 suggests an interesting feature of the expected results of the ITAM process. The suggestion is, that organizations expect improvements in efficiency and effectiveness. However, the expectations are commonly not met as they were planned. This is a result of the broadness of the required implementations and required re-designs alongside the implementation. Equally is suggested, that organizations are to keep on pursuing

these results due to the already received "quick wins" proving the effectivity of the ITAM. A final point brought up is that the actual best practices of ITAM are often implemented last. This can be reasoned with the scope of the best practices, which extend to the strategical level of an organization, and often provide results only in a long time span. (ISO/IEC 19770-1 2012: 34.)

IAM recommends that an organization shall have a variation of strategies developed to support the asset management. These strategies can include organization-specific plans, but should also include ones for management of critical assets, for economic end-of-life, and for a general long-term planning. Long-term planning is tied to management of critical assets, as there should not become a situation where for example a software should be replaced just before the hardware would become replaceable. Economic end-of-life of an asset is stated to be a known challenge in many organizations. Understanding when an asset's performance, required costs and reliability have converted the asset to a negatively impacting asset is not definitive unless it is defined in a strategy. Replacing an asset in its economic end-of-life makes the funding forecasting easier as well. The ITAM's strategical aspect yields a one additional argument for proposing an organization's senior management to lead the organization's asset management. (IAM 2015: 44.)

5.3 Proposed Implementation

To start the likely months lasting development of the organization-wide, deeply integrating, remarkably broad ITAM for an organization, one should at first find answers to two highly organization-specific questions: what is the depth of the detail required, and what is the breadth of components (Green & Helstrom 2011: 368–369). These two questions are to scope the organization's ITAM in a great extent. After the scope is clear, the organization can move on to plan and design the core ITAM processes. These four processes – configuration management, change management, incident management and financial management – each have a major role in the shaping of the ITAM. The processes are explained in more detail in the chapter 2.2.1.

The open-ended planning and designing of ITAM can be supported with the several SAM processes deriving from ISO/IEC 19770-1 which each of have been shown in the Table 3. The process group "Organizational Management Processes for SAM" includes in total eight different processes which assist in shaping the ITAM to a thoroughly acknowledging in terms of management and design. The following process group "Core SAM Processes" provides eleven processes to further support in the ITAM processes such as configuration management and financial management, but also to consider otherwise easily excluded aspects of service, security and contract management. Finally ISO/IEC 19770-1 covers the group of SAM processes "Primary Process Interfaces for SAM" also consisting of eight processes. These processes, just like "Core SAM Processes", have overlapping features with the ITAM processes. Moreover they extend the coverage by detailing the various aspects of assets' life cycle. The exact associations between the SAM processes and the tiers have been detailed in the Tables 3–5. By following the SAM processes provided in the guidance of the related standard, the organization should be able to more effortlessly achieve the conformity to the standardization. One should also note, that the implementation of the processes can be outsourced, which is up to the organization to be decided if it suits them better. (ISO/IEC 19770-1 2012: 7–33.)

Once the vast design is done, the ITAM processes should direct towards the requirements the organization has from the tools involved in ITAM. When considering the tools, the organization should have expectations for the initial required work to achieve static inventories, determine the tasks which need to be automatized, and have assumptions of the desired analytical outputs from the asset management data. Tools of ITAM have been discussed more in the chapter 2.2.2. At this early stage a tool to support data discovery, data gathering and data acquisition is recommended to be harnessed into use, as it will become almost an essential during the static inventory's establishing as described below.

When we place the four tiers of ISO/IEC 19770-1 among the ITAM processes, there is a direct association between tier 1 and configuration management. By the use of configuration management the assets of the organization can be identified, verified, and become controlled and maintained as configuration items. This corresponds to the tier 1's requirement of having a knowledge of the assets (ISO/IEC 19770-1 2012: *vi*). Although based

on Barry *et al*. (2011: 91–92) an additional data handling is not a must have with the configuration items, in this study we additionally highlight as a step the possibility to add the optional data handling due to the diversity of configuration items' data. This can be done as part of the data gathering – a task which can be supported with for example discovery methods of domain-connected assets and surveys for undiscoverable assets. The gathering of traditional IT assets must be expanded to the software contracts and licenses. Contracts and licenses are expected to be largely manually gathered, which may cause challenges, but shall still be taken care of as part of the tier 1 stage (ISO/IEC 19770-1 2012: 34).

Furthermore with the available configuration items the initial CMDB can be formed. This static inventory becomes the base of the ITAM. Although configuration management provides the core guideline for establishing the static inventory, the history and financial properties of assets are also needed for the configuration items of static inventory (Bonham 2004: 145). As Bonham (2004: 145) recommends, using a single inventory to form the CMDB would be the most optimal decision when the organization is consistent. The target company's organization suits for this purpose, which is why a single-inventory-based master CMDB is used in the proposal. This changes the multi-inventory schema shown in Figure 3 to a single-inventory-based schema with a direct conversion to a CMDB, as illustrated in the Figure 9. The single-inventory-based structure more effortlessly enables the advantages layered asset description framework offers as described in the chapter 2.2.4.

By wrapping the tools chosen for ITAM around the static inventory and the involved processes, the data of the static inventory can be analyzed for the first time. The tools' functionalities should be able to work with the static data in the same manner the functionalities would work with constantly changing data. With the tools the first quick wins can be delivered with the likelihood of disclosing the many assets which had not been managed prior to this. The quick wins and the control of asset management are an emblematic indication for the milestone of tier 2 (ISO/IEC 19770-1 2012: *vi*).

By combining the remaining three ITAM processes, the tools and the static inventory, the static inventory has all the potential to become an inventory which becomes fed by new data having its origins in for example incident and financial sources, but also when an asset or its associations such as an ownership changes. These additions conclude to converting the static inventory into a dynamic inventory. In practice this simply described step requires that each of the ITAM processes – and SAM processes preferably as well – are put into action from their design stage. The dynamic inventory again corresponds to yet another tier, being tier 3. Tier 3's achievability demands the operability of the asset management with an improved efficiency and effectiveness (ISO/IEC 19770-1 2012: *vi*).

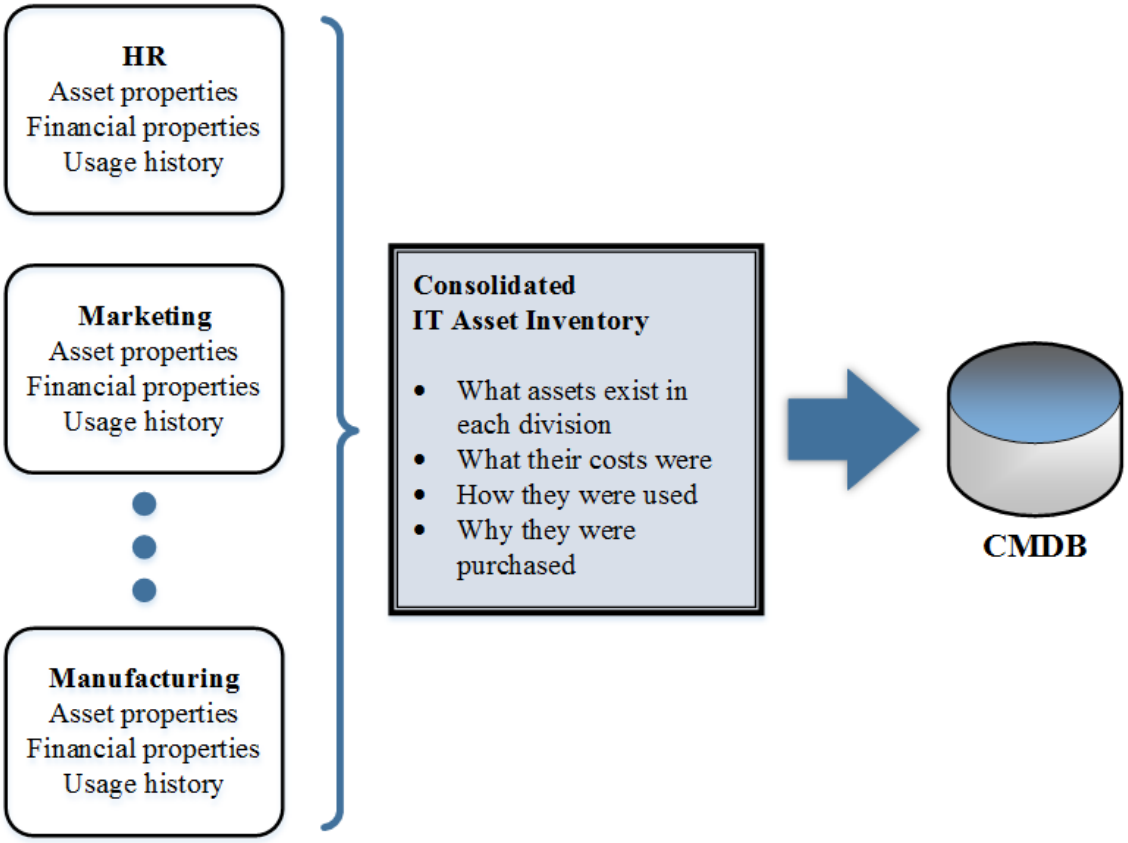


Figure 9. A single-inventory-based CMDB can be used as the organization's structure is consistent.

A thoroughly designed dynamic inventory for IT assets has been put into practice at this stage. Between the tiers 3 and 4 are only a few additional tasks, but more importantly the design of the tiers 1 and 2 will be put into a test. Changes to the initial steps can still be easily implemented, which often is not the case for a system in a production use. The conformity of the ITAM and its processes should be assessed at this point. The assessing should be done internal, as the ITAM in total may still receive changes until the initial auditioning. An efficient way to assess the SAM processes of ISO/IEC 19770-1 (2012) is to follow the expected outcomes of them. This again is not a requirement for a standardization, as the ISO/IEC 19770-5 (2015: 12) points out that if the received outcomes can be demonstrated, and are sufficient when contrasted to the requirements, that will be sufficient. For the full conformance there are two additional required assessments to be done besides the assessment of SAM processes. One is that a SAM process area extending to more than one tier shall be "interpreted correspondingly for assessment of each tier". The other requirement is that during the assessment, the outcomes need to be taken into account, and if there are any exceptions in the objectives that should be met, the assessor must explain the reason or reasons why the exception is allowed in the form of a documentation (ISO/IEC 19770-5 2015: 12).

On top of the normative guidance, the assessment should find neutral opinions for a set of questions, which should challenge the team working on ITAM (ISO/IEC 19770-5 2015: 13). These questions may reveal notable problems which might be discovered only after the commissioning of ITAM. The questions should include at least the following:

- Is there a clear direction in the ITAM's development?
- Is there a clear ownership for ITAM?
- Is ITAM reasonably scoped?
- Are there clear roles and responsibilities around ITAM?
- Are the usage rights of the assets and such understood by the management?
- Have there been done significant compromises due to resources?
- Does ITAM have capability to be used in the decision making?
- Is sufficient documentation of the development created and planned?

An ITAM that has gone through an internal assessment and satisfied the requirements can be re-defined to be in full conformance. At this point the strongly relevant process for IT asset acquisition should be tied to the ITAM. While the IT asset acquisition ordinarily already exists in some form in an operative organization, its process might become revised during the design-phase of ITAM. IT asset acquisition, a rather large subject as itself, involves the addition of IT assets to the ITAM, but often decommissions too. In this study we do not focus on going through the IT asset acquisition process suitable for the target company, as this has been done already earlier. A study authored by Pääkkönen (2015) called "Ohjelmistonjakopisteen perustaminen etäverkkopisteelle" ("Setting up a software distribution point to remote network") has provided a guideline for the target company, which can be integrated to a parent asset management system such as the ITAM of this study is.

Like acquisition, decommission of an asset is a remarkably important step in its life cycle. ISO/IEC 19770-1's process called "Retirement process" is designed for this purpose. With the assumption of the process already being demonstrably sufficient according to the done steps, the retirement process should cover the organization's activities for decommissioning its assets (ISO/IEC 19770-1 2012: 32–33). By demonstrating the conformance to the retirement process, the organization shall be able to have policies and processes for the following scenarios:

- Deployed software are removed from a hardware as part of the decommissioning.
- Licensed and otherwise redeployable software are identified as part of the decommissioning.
- Any asset transferred to an internal or external party is treated as a decommissioning asset.
- Assets and licenses which are not to be redeployed shall be properly disposed.
- Any of the mentioned changes are projected to the changelog or similar of an asset to support the auditability. (ISO/IEC 19770-1 2012: 33.)

Finally the ITAM should receive an operative surveillance program. Surveillance program is done to ensure the conformance's continuing, and the program shall be accepted by the assessor as part of the compliance certification for full conformance. The surveillance program's primary task is to monitor the performance of the many processes put into practice (ISO/IEC 19770-1 2012: 3). After this the ITAM can be advertised as the best-in-class ITAM. Besides the best-in-class ITAM stage of deployment, the complete practices of ITAM and SAM are to be fully integrated into the organization's strategic planning. An ITAM with all of the above detailed properties meets the requirements of the tier 4 of ISO/IEC 19770-1.

ITAM's establishing is largely supported by the topics of ISO/IEC 19770-1. The remaining standards in the study, ISO/IEC 19770-2, ISO/IEC 19770-3, ISO/IEC 19770-4 and ISO/IEC 19770-5, may be seen as performance improving potentials, each being able to be integrated to an existing ITAM. While ISO/IEC 19770-2, ISO/IEC 19770-3 and ISO/IEC 19770-4 can be implemented completely separately from ISO/IEC 19770-1, the terminology and vocabulary of ISO/IEC 19770-5 should be obeyed already since the ISO/IEC 19770-1's early stages. An unambiguous documentation may become a key factor for an organization to adapt into the new practices. The remaining standards' development could be taken into account during the design of the initial ITAM, but by doing so, the already challenging design and development task becomes yet more demanding.

ISO/IEC 19770-2 has descending associations to ISO/IEC 19770-3 and ISO/IEC 19770-4. When any attributes or such of ISO/IEC 19770-2 are included in the entitlement schemas of ISO/IEC 19770-3, the used properties must conform to the requirements of ISO/IEC 19770-2, whereas the resource utilization measurements' naming convention includes the SWID tag files' names as part of the .rum-files (ISO/IEC 19770-3 2016: 21; ISO/IEC DIS 19770-4 2016: 8.). This would suggest the implementation of ISO/IEC 19770-2 prior to the implementation of ISO/IEC 19770-3 and ISO/IEC 19770-4.

What challenges the conformance to the standards ISO/IEC 19770-2, ISO/IEC 19770-3 and ISO/IEC 19770-4 is their strict requirement to have each of their own ITAM supporting instrument supported by their linked software asset, being respectively a SWID tag

file, an entitlement schema and a resource utilization measurement file (ISO/IEC 19770-2 2015: 3; ISO/IEC 19770-3 2016: 8; ISO/IEC DIS 19770-4 2016: 4–5). Due to the relatively recent evolvement of ISO/IEC 19770 standards, the conformance for the standard family is far from desired at both product-level and vendor-level. This results in the need of creating the own ITAM instruments at the consumer-end, which supposedly reduces the likelihood of achieving the total ISO/IEC 19770 support among the consumers.

Figure 10 illustrates the proposed implementation for ITAM. The graph differentiates the ITAM processes, tiers, standards and the stages of the ITAM along the development. The implementation is supported by highlighted action points deriving from asset management's, ITAM's and SAM processes' best practices. As ISO/IEC 19770-5 does not belong to the scope of conformance, it is separated from this illustration.

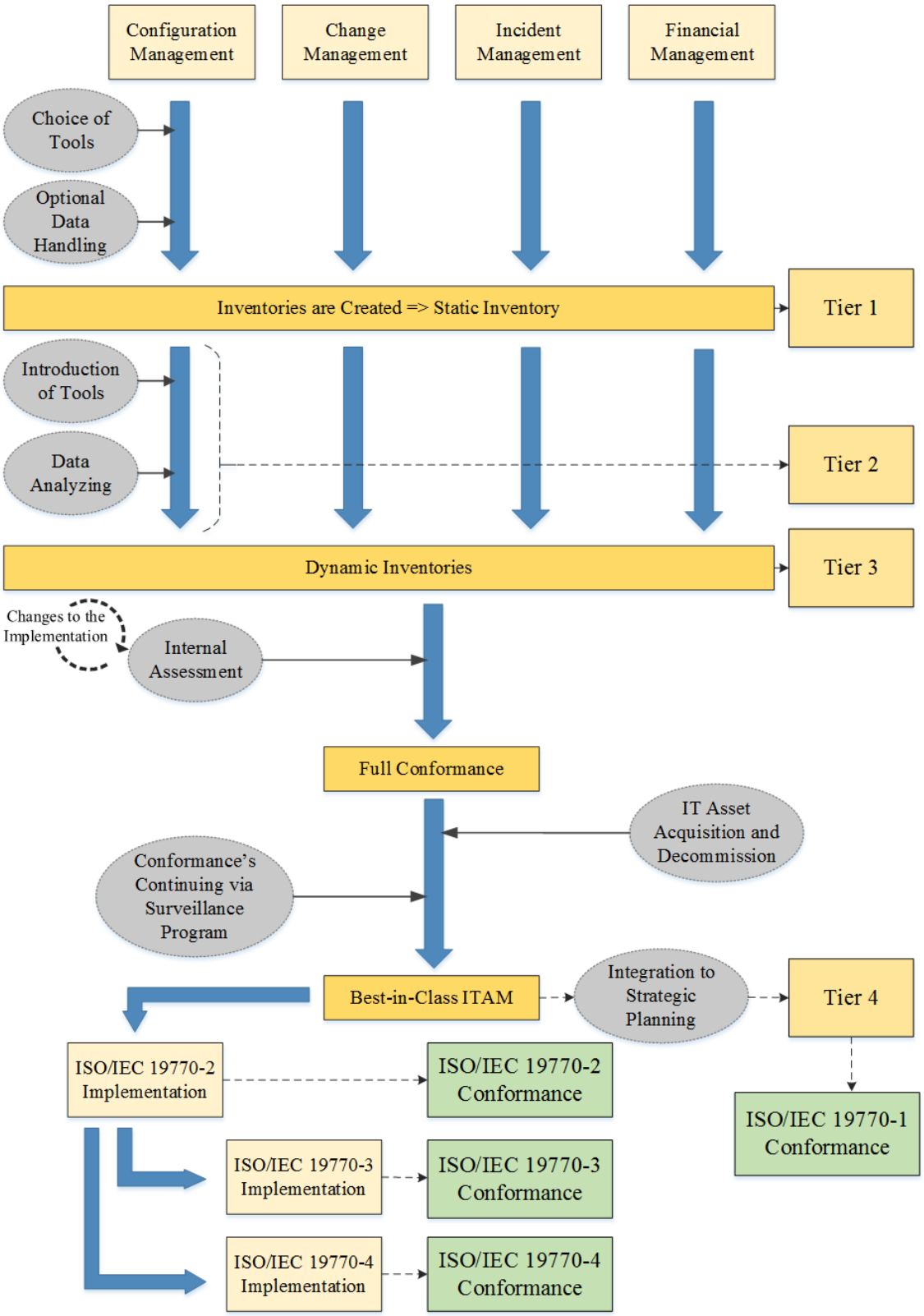


Figure 10. The proposed guideline for ITAM's implementation.

5.4 Benefits and Liabilities

In the fourth subchapter the proposed guideline is evaluated with the aspects of how it can benefit the target company, but also by taking into account what liabilities the implementation proposed by the guideline yields.

Asset management in total can lead to significant savings when done properly. Helstrom & Green (2011: 355) mention a model, where a freshly started asset management program could lead up to 30% cost reductions within the first year of operation. The following five years would further benefit the enterprise with continuing 5–10% cost reductions. Asset management's operability in an ICT company is largely dependent on the functionality and efficiency of the ITAM. The most significant savings can be earned by reusing the existing assets. Processes for effectively discovering and reusing such assets become essential, which is backed up by an alongside given estimation: ITAM is 80% processes, 20% tools. This underlines the importance of proper planning and designing. (Helstrom & Green 2011: 355.)

Enterprises can make several decisions in order to implement an enterprise asset management which fits the company's goals, resources, needs, culture and other desires. Compromises are what risk the effectiveness of the asset management and should thus be avoided. Another extreme is an overly optimistic or frugal attitude towards the assets' performance and life expectancy. An analysis by the tools for ITAM could even unveil assets which cost the company more than replacing it (IAM 2015: 44). Some of the tools the chapter 2.2.2 highlights could provide models for building realistic estimates for the length of the assets' life cycle. One should also note, that not everything is designed to become recycled within the company. Bonham's (2004: 149) general rule is, that asset should not be acquired as a recyclable item unless there will be at least three committed holders for the asset by its life cycle.

The design of the proposed ITAM is being based on a single-inventory model, where CMMS becomes the primary CMDB directly. Bonham (2004: 146) supports the use of single-inventory structure with the decreased risk of stranded assets in consequence of

enhanced asset recycling. This is added with the increased chance of receiving benefits from vendors and service providers as a result of consolidated processes. Additionally by having a consolidated inventory in place, reacting to changes

The proposed guideline for ITAM is built so, that it can be implemented without pursuing the related standards from the ISO/IEC 19770 family of standards, but effective results can still be achieved. Although ISO/IEC 19770-1, the standard which the most closely supports the development of ITAM, can be segregated from the development of the ITAM's development, the conformance to the standard especially in its lower tiers should not require a significant further effort. Many of the processes detailed in ISO/IEC 19770-1 are naturally developed along ITAM, and the standard's processes mostly take care of that no essential parts of ITAM are omitted. Nevertheless when aiming for a standardization, an initial audit is required, and any exceptions to the requirements should be handled carefully before pursuing the formalization. The organization should additionally confirm their legal entity type is applicable for a standardization. In the case of the company part of the study, a single legal entity is applicable and does not require any special arrangements (ISO/IEC 19770-1 2012: 1).

The tolerable amount of work for standardization is not expected to be the case with the other standards from the family. As reasoned in the previous chapter, achieving a full conformance to the standards ISO/IEC 19770-2, ISO/IEC 19770-3 and ISO/IEC 19770-4 may require an insuperable amount of work until the vendors and producers of the software and services support the standards in question. Prior to that, enterprises may prepare for the standards by preparing tools suited for the management of the instruments of the standards.

Although ITAM is supposedly a system supported by the best available automation, the system is still dependent upon regular monitoring and administering. These cause obvious liabilities, but are in place only to maintain the operability and effectiveness of the program. As discussed earlier, an involvement of a senior management level is also required

to authorize the ITAM among other benefits. Other personnel to work around ITAM during its development and maintenance stages include developers, administrators and experts able to adjust and integrate ITAM to the changing environment.

5.5 Post-implementation

After the ITAM has been implemented and initialized into use, it should not become treated as a system in maintenance by itself. A recently started system still requires some post-implementation steps which are discussed in this chapter. The surveillance program for conformance's continuing as detailed in the chapter 5.3 is possibly the most important and efficient way to maintain the ITAM, but not every post-implementation step requires a continuous operability as there are some one-time executed tasks as well. None of post-implementation tasks discussed in this chapter exactly falls to the requirements of the ISO/IEC 19770's standards, but are nevertheless strongly suggested steps in the ITAM's implementation.

Although it is suggestable that a change in ITAM is communicated to the users and other stakeholders of the assets already prior to the implementation of the practices (IAM 2015: 40), it needs to be clearly communicated and documented especially after the implementation. Members of the entity running ITAM must be aware of the system, although the members do not actively contribute for or work with the system. A consciousness of the system in the background can preempt in future challenges, such as reoccurrence of assets becoming stranded.

As the consolidated inventory based CMDB becomes the primary point for adding and decommissioning assets, the process which involves the asset's handing in and out from the organization becomes managed by the same authority. This centralization offers several possibilities as detailed in the chapter 2.2. Without actively pursuing towards the possible benefits of centralization, a little can be expected. A dedicated responsible such as a person generally doing the asset acquisitions should attempt to negotiate better contracts for the assets acquired.

Finally, although a freshly developed system for managing IT assets has just been taken into use, ITAM's future should be considered. Not long ago enterprises kept account of assets by a pen and a notebook, only to move to electronic notebook and spreadsheet options. Unnecessary to detail, IT has evolved and will evolve in a pace which is only merely graceful towards static environments. Some organizations might have a planning system in place or upcoming, which could be a natural platform to integrate the asset management and financial management systems of the organization (Barry *et al*. 2011: 107). Another way to evolve ITAM would be to plan a more mobile system. Mobile systems would be more effortlessly accessible from a remote site, include quickly processable labels such as remote identifiers, and communicate through geographic information system to their parent sites (McGlynn & Fenhagen 2011: 393–395).

6 ANALYSIS OF RESULTS AND FINDINGS

An ICT company pursuing for an ISO/IEC 19770 level of ITAM should at first pursue for an organization-wide ITAM. Adding the level of standardization comes as parts. ISO/IEC 19770-1 which is the primary ITAM development supporting standard can be achieved in four tiers of which the fourth of the tiers equates to the standard's requirement. ISO/IEC 19770-2, ISO/IEC 19770-3 and ISO/IEC 19770-4 can each be implemented completely separately from each other, but preferably by having ISO/IEC 19770-2's requirements fulfilled prior to moving to the subsequent standards. These three standards do not have a tier-based structure which is why they are to be implemented as whole pieces. ISO/IEC 19770-5 does not belong to the scope of conformance, as it serves as a guiding standard for the others standards in the standard family. The remaining standards of ISO/IEC 19770 family of standards have no published versions available at the time the study was conducted which is why they are not taken into account when planning ITAM in this study.

The proposed implementation allows the organization to choose a scope of ISO/IEC 19770 to pursue. Organization's size, field of business, extensibility, and for example the functioning of current practice to manage IT assets are all properties, which are organization-specific and make a difference when planning the ITAM's scope. In addition, ISO/IEC 19770 gives a choice of freedom in several practical matters such as the choice of tools and order of implementation. The proposed implementation guideline, as is, is not expected to suit for small nor large ICT companies or organizations, but mid-size ICT companies or organizations.

The study's theoretical part was divided into two. The first part consisted of a literature research, where articles, books and other literature concerning asset management and its subfields namely enterprise asset management and ITAM were discussed. The second part of the theory detailed the ISO/IEC 19770's broad family of standards focusing on the five first sequential standards being the ones having a published version at the time the study was conducted. Although the theory resulted into a relatively large part of the study, each part of the theory became essential when forming the guideline for the ICT company

about ITAM's implementation. Between the theory and the development of ITAM guideline was a chapter to define the used research method, action research. Action research was used in this study to research the requirements of the target company. Two members of the target organization acting in key positions concerning asset management were interviewed with an unstructured set of questions. The information was added by the author's knowledge of the domain. The gained knowledge became helpful when forming the more general guideline for ITAM, but also when finding exact needs for the target company when designing the proposed implementation. Altogether the parts of the study supported each other without exceptions. The study achieved the set targets with results encouraging for low threshold adaption with an incentive for a higher outcome in the form of international standardization.

7 CONCLUSIONS

The goal of this thesis was to produce a guideline for an ICT company about how the company could manage the IT assets of the company in the most efficient way. The study's research question was "*how an ICT company can achieve the ISO/IEC 19770 level of ITAM?*" which is answered here according to the information detailed in the preceding chapters. The study was done in two parts. The first part was to do a literature review about asset management with a focus on ITAM and to study the ISO/IEC 19770 standards' parts 1–5. The second part, conducted as an action research, was to develop the ITAM's proposed implementation guideline and to evaluate it. The theory part of the study resulted into a multifaceted literature study of asset management and especially ITAM, and into a comprehensive review of the related standards. Based on the extensive theory, and learned enterprise-world circumstances through the conducted current state analysis part of the action research, an acknowledging guideline for ITAM's implementation could be developed. This guideline is delivered to the study's target company as a proposal for how to implement ITAM within the target company's organization.

ISO/IEC 19770 level of ITAM can be achieved by following the given proposed implementation guideline detailed in the chapter 5.3 which presumes that the requirements of the related standards are followed along the ITAM's development. The conformance to the related standards can be developed and achieved in parts. Additionally the chapter 5 analyzes the expected problems enterprises face in asset management, the guideline's benefits and liabilities, and what post-implementation tasks there remains after the guideline's steps. The guideline was developed so, that it does not bind its follower on pursuing the ISO/IEC 19770 standards while still offering a comprehensive strategy for implementing an ITAM system for an organization. The guideline was constructed from the parts of existing literature of asset management, enterprise asset management and ITAM, and completed with the process-based practices and a suggested structure based on primarily the documentation of ISO/IEC 19770-1. Based on the guideline, we may suggest the target company to pursue the standardized ITAM in order to improve the utilization of the company's IT assets. The achievability of the ISO/IEC 19770 level of ITAM is

expected to be a challenging and time-demanding task with an opportunity for high rewards. The study suggests, that a careful planning, designing and a continuous observance to the related processes are essential for achieving the best-in-class ITAM.

The previous literature about the subject consists of Wright's (2011) software life cycle management, which covers the ISO/IEC 19770's part 2, and considers the part 3 and the literature about ISO/IEC 20000, the standard for IT service management, which has some aligned elements to the ISO/IEC 19770 standard. Other previous literature, which feature the topics of asset management, enterprise asset management or ITAM, does not consider the standards of ISO/IEC 19770 family of standards. Instead the literature defines the terms and their concepts without referring to the ISO/IEC 19770's standards although references to other standards may exist. This thesis could be interposed between the non-standard referenced literature of ITAM and the ISO/IEC 19770 considering the covered literature and the overall covering of the released documentation of the standards.

Furthermore the study can be continued by both parties involved in the action research. The continuously developing ISO/IEC 19770 will expand in the future and new editions of the existing parts will be released over time. The planned parts, which did not have a released version as of 12/2016, are likely to offer enterprises new ways to develop and expand their ITAM as soon as they are released, and to extend the existing standards as technical reports. The next editions of the existing parts should specify the concepts to a more relevant format and include additions to the already released material. The target company in the study can start to utilize the delivered guideline in practice to achieve the full benefits of the improved ITAM. The adaption of ITAM should be monitored closely by the surveillance program and by for example doing a new iteration of the action research to find out remaining or arisen problems. ISO/IEC 19770's applicability to businesses of different field could be investigated, as in this research we focus primarily on the field of ICT.

REFERENCES

Barry D., B. Helstrom & J. Potter (2011). Information Management and Related Technology. In: *Asset Management Excellence. Optimizing Equipment Life cycle Decisions*, 89–132 pp. Eds. J.D. Campbell, A.K.S. Jardine & J. McGlynn. 2nd ed. Boca Raton (FL), US: CRC Press. ISBN 978-0-8493-0300-5.

Bonham, Stephen S. (2004). *IT Project Portfolio Management*. Norwood, US: Artech House Books. 285 pp. ISBN 978-1-58053-782-7.

Campbell, J.D., A.K.S. Jardine & J. McGlynn (2011). *Asset Management Excellence. Optimizing Equipment Life cycle Decisions*. 2nd ed. Raton (FL), US: CRC Press. 474 pp. ISBN 978-0-8493-0300-5.

Checkland, Peter (2000). Soft Systems Methodology: A Thirty Year Retrospective. In: *Systems Research and Behavioral Science*, 11–58 pp. Ed. M.C. Jackson. 17th volume. John Wiley & Sons, Ltd. ISSN 1092-7027.

Davis, Robert (2012). *An Introduction to Asset Management*. Capenhurst, Chester, UK: EA Technology Ltd. 32 pp. ISBN 978-0-9571508-3-6.

Frolov V., L. Ma, Y. Sun & W. Bandara (2010). Identifying Core Functions of Asset Management. In: *Definitions, Concepts and Scope of Engineering Asset Management*, 19–30 pp. Eds. J.E. Amadi-Echendu, K. Brown, R. Willett & J. Mathew. London, UK: Springer. ISBN: 978-1-84996-178-3.

Green Ron & Brian Helstrom (2011). Information Technology Asset Management. In: *Asset Management Excellence. Optimizing Equipment Life cycle Decisions*, 363–378 pp. Eds. J.D. Campbell, A.K.S. Jardine & J. McGlynn. 2nd ed. Boca Raton (FL), US: CRC Press. ISBN 978-0-8493-0300-5.

Hastings, Nicholas A.J. (2010). *Physical Asset Management*. 1st ed. London, UK: Springer-Verlag. 370 pp. ISBN: 978-1-84882-751-6.

Helstrom, Brian & Ron Green (2011). Information Technology Service Management Life Cycle. In: *Asset Management Excellence. Optimizing Equipment Life cycle Decisions*, 351–362 pp. Eds. J.D. Campbell, A.K.S. Jardine & J. McGlynn. 2nd ed. Boca Raton (FL), US: CRC Press. ISBN 978-0-8493-0300-5.

IAM (The Institute of Asset Management) (2015). *Asset Management – an Anatomy*. Bristol, UK: The Institute of Asset Management. 84 pp. Available at: http://www.theIAM.org/AMA. ISBN 9-781908-891129.

ISO (2016). International Harmonized Stage Codes. [online]. [Referred on 7.11.2016]. Available at: http://www.iso.org/iso/home/standards_development/resources-for-technical-work/stages_table.htm.

ISO (2017a). International Organization for Standardization. [online]. [Referred on 16.3.2017]. Available at: https://www.iso.org.

ISO (2017b). ISO/IEC WD 19770-8. [online]. [Referred on 19.6.2017]. Available at: https://www.iso.org/standard/72588.html.

ISO (2017c). ISO/IEC 19770-3:2016. [online]. [Referred on 20.5.2017]. Available at: https://www.iso.org/standard/52293.html.

ISO (2017d). ISO/IEC PRF 19770-4. [online]. [Referred on 5.6.2017]. Available at: https://www.iso.org/standard/68431.html

ISO/IEC 19770-1 (2012). *Information technology – Software asset management*. Part 1: Processes and tiered assessment of conformance. Edition 2. 80 pp.

ISO/IEC 19770-2 (2015). *Information technology – Software asset management*. Part 2: Software identification tag. Edition 2. 72 pp.

ISO/IEC 19770-3 (2016). *Information technology – IT asset management*. Part 3: Entitlement schema. Edition 1. 62 pp.

ISO/IEC 19770-5 (2015). *Information technology – IT asset management*. Part 5: Overview and vocabulary. Edition 2. 19 pp.

ISO/IEC DIS 19770-4 (2016). *Information technology – IT asset management*. Part 4: Resource utilization measurement. Edition 1. 34 pp.

Kananen, Jorma (2013). *Design Research (Applied Action Research) as Thesis Research*. *A Practical Guide for Thesis Research*. Jyväskylä: JAMK University of Applied Sciences Library. 232 pp. ISBN: 978-951-830-261-5.

Kemmis Stephen & Robin McTaggart (2005). Participatory Action Research. Communicative action and the Public Sphere. In: *The Sage Handbook of Qualitative Research*, 559–603 pp. Eds. Norman K. Denzin & Yvonna S. Lincoln. Thousand Oaks (CA), US: SAGE Publications, Inc. ISBN 978-0-7619-2757-0.

Koshy, Valsha (2005). *Action Research for Improving Practice: A Practical Guide*. New Delhi, India: SAGE Publications Ltd. 166 pp. ISBN 978-1-8486-0081-2.

Kumar, S. Anil & N. Suresh (2007). *Production and Operations Management*. *With Skill Development, Caselets and Cases*. 2nd ed. New Delhi, India: New Age International. 284 pp. ISBN: 978-81-224-2425-6.

Lin C., C. W. Lan, J. Ye & Y. C. Wu (2013). *A Design on Smart Enterprise Asset Management*. 2013 IEEE 10th International Conference on e-Business Engineering (ICEBE) (Coventry): IEEE. 456–460 pp. doi: 10.1109/ICEBE.2013.71. ISBN 978-0-7695-5111-1.

McGlynn, Joel & Don Fenhagen (2011). The Future of Asset Management Solutions – Consolidation, Capability, Convergence. In: *Asset Management Excellence. Optimizing Equipment Life cycle Decisions*, 391–400 pp. Eds. J.D. Campbell, A.K.S. Jardine & J. McGlynn. 2nd ed. Boca Raton (FL), US: CRC Press. ISBN 978-0-8493-0300-5.

Mohseni, M. (2003). *What does asset management mean to you?* 3rd ed. 2003 IEEE PES on Transmission and Distribution Conference and Exposition (Dallas): IEEE. 962–964 pp. doi: 10.1109/TDC.2003.1335069. ISBN 0-7803-8110-6.

Pääkkönen, Anton (2015). *Ohjelmistonjakopisteen perustaminen etäverkkopisteelle*. University of Vaasa. Software Engineering. Bachelor's thesis [printed].

Reponen, Tapio (1992). Action Research in Information Systems Strategy Formulation and Implementation. In: *Action Research in Management Information System Studies*, 52–64 pp. Ed. Liisa von Hellens. Turku: Publications of the Turku School of Economics and Business Administration. ISBN 951-738-575-7.

Stringer, Ernest T. (1999). *Action Research*. 2nd ed. Thousand Oaks (CA), US: SAGE Publications, Inc. 229 pp. ISBN 0-7619-1716-3.

Wapice (2016). Wapice Ltd. [online]. [Referred on 7.11.2016]. Available at: https://www.wapice.com/about-us/wapice.

Wright, David (2011). *Software Life Cycle Management Standards*. *Real-world Scenarios and Solutions for Savings*. Cambridgeshire, UK: IT Governance Publishing. 193 pp. ISBN: 978-1-84928-205-5.

Zutec (2016). Zutec Cloud Solutions [online]. [Referred on 29.11.2016]. Available at: http://www.zutec.com/external-sites/cloud/zutec-cloud-solutions.