Frequently Asked Questions about the 3rd edition of the ISO ITAM standard (ISO/IEC 19770-1:2017 IT Asset Management – Requirements)

Version of 27 June 2018 – © 2018 David Bicket

This is a FAQ sheet prepared by David Bicket (dpb@m-assure.com), a co-editor of the revised ISO ITAM standard, based on questions received personally or raised in on-line discussions. It will be updated and extended from time to time. This document, or updates, can be downloaded from www.m-assure.com. It may be reproduced by others under creative commons licensing if attribution is given.

Table of Contents

1. What are the differences between editions 2 and 3 of ISO ITAM? 1
2. Where have all the edition 2 processes gone? 2
3. Why has the edition 2 guidance been removed from edition 3? 2
4. How do you implement ISO ITAM? 3
5. How do you get certified against ISO ITAM? 3
6. Why does edition 3 require so much effort to understand? 4
7. Why is risk management both in clause 6 and in the optional add-ons for clause 8? 5

1. What are the differences between editions 2 and 3 of ISO ITAM?

The major differences are:

- **Presentational:** ISO ITAM is a 'Management System Standard' (MSS), and ISO now requires all MSSs to use a common high-level structure and to include certain common text. This is to facilitate the integrated use of different MSSs, such as with information security (27001), quality management (9001), and service management (20000-1).
- **Objective-driven not outcome-driven:** This represents an evolution from edition 1 (in 2006), through edition 2 (in 2012) to edition 3 (in December 2017). Although the standard was originally developed as an MSS (based on the service management standard), the first edition had to be rewritten to specify requirements as 'outcomes' instead of 'objectives' because of the internal requirements of the committee where WG21 is based (which 'didn't do MSSs' at the time). For example, one outcome was 'the hardware inventory including locations is verified at least 6-monthly…'. Unfortunately, this approach was effectively a 'product specification', and did not work well for MSS certification bodies. Edition 2 allowed a choice between assessment based on the earlier outcomes or just on objectives. For example, the overall objective corresponding to the previous example outcome (plus many more detailed outcomes) was 'to ensure that records reflect accurately and completely what they are supposed to record…'. Edition 3 eliminates the detailed outcomes and relies solely on the overall objectives.
- **Explicit coverage of major control issues.** There is now more explicit coverage of topics such as:
    - Outsourcing and services

    - Mixed responsibilities between the organization and its personnel
    - Traceability of ownership and responsibility
    - Audit trails of authorizations and execution of authorizations
- **ITAM vs SAM:** In my view, this is a purely a question of usage, rather than content, but should be mentioned. Edition 2 was SAM requirements; edition 3 is ITAM requirements. However, the scope of edition 2 included related assets which were all other assets with characteristics which are necessary to use or manage software, which clearly included hardware.

2. Where have all the edition 2 processes gone?

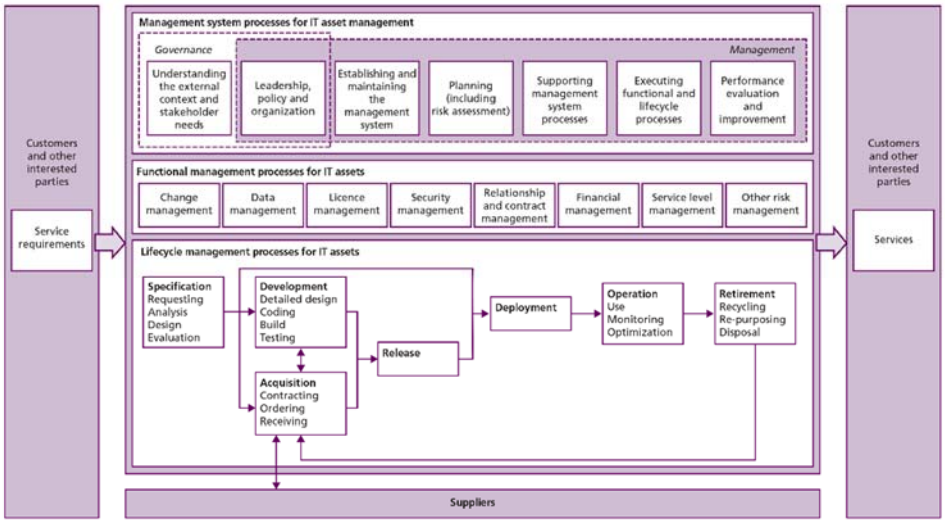
They are still all there, but a number have been moved to Annex A. To explain: Edition 2 introduced the concept of tiers, so that an organization could get certified for critical processes (especially tier 1 for trustworthy data) without being certified for everything. This was accomplished by including all the core SAM processes and life cycle processes in the main body of the text, but with tables to indicate which objectives and outcomes were included in which tiers. Edition 3 has retained the concept of tiers, but it has been done in the same way as ISO/IEC 27001, where all (additional) objectives are listed in Annex A. The organization needs to decide which objectives are to be covered by its IT asset management system, and document this in a 'Statement of Applicability', the same as for ISO/IEC 27001.

3. Why has the edition 2 guidance been removed from edition 3?

There are two different ways of answering this question.

1. The technically specific answer: The detailed outcomes included in edition 2 were never intended as guidance, but were rather included as one possible way of determining conformance. (See also the explanation of 'objective-driven not outcome-driven' above.) These are not appropriate for a proper MSS, so they have been dropped from edition 3.
2. The more general answer: A 'requirements' document such as 19770-1 is supposed to cover just requirements. Guidance is a much broader topic, and there are many ways of getting such guidance for 19770-1:
    a. ISO guidance. It is possible for WG21 (the working group responsible for ISO ITAM) to produce another standard on 'guidance for the implementation of ISO/IEC 19770-1:2017'. This has not yet happened, but anyone wishing to work on it should coordinate with the WG21 convener. There is also a useful standard ISO 55002 which should be published sometime in 2018, which is 'guidance for the implementation of ISO 55001:2014'. Since 19770-1 includes most of the text of 55001, this should be highly useful once it is available. A third ISO source which can be mentioned is edition 2 of ISO/IEC 19770-1, with its detailed outcomes. While this was not intended as guidance, it can be used in this way.

b. Commercial guidance. Anybody can publish their own guidance on the use of any standard, and this is the main expected source of guidance on the use of edition 3. I am co-author of one such publication, the ITIL Guide to Software and IT Asset Management, edition 2, published in January 2018, which covers the new ITAM standard. The diagram below about 19770-1:2017 is from that Guide.



Reproduced with kind permission from The Stationery Office, ITIL Guide to Software and IT Asset Management, Bicket and Rudd, 2018. ISBN 9780113315482

4. How do you implement ISO ITAM?

The question is simple; the answer is not. Some guidance is given in the ITIL SAM/ITAM Guide (see above). In short, it depends on many factors, such as:

- Your objectives with ITAM, and scope (e.g. just for specific publishers or platforms?)
- The current state of ITAM in your organization (e.g. tools, processes, people skills)
- The level of management support and resources available
- Organizational implications (e.g. legal and regulatory environment especially for multi-nationals and regulated industries; level of organizational centralization vs decentralization)
- Who might help you implement it (e.g. in-house only; with a tool provider; with consultants; or using a managed service provider?)

5. How do you get certified against ISO ITAM?

Firstly, it needs to be clarified that ISO/IEC 19770-1 is for organizations, so the question is how an organization can be certified against ISO ITAM. There are multiple threads to answering this question:

- Anyone can certify. In most countries, legally anyone can certify an organization against 19770-1, including e.g. a driver or a cleaner. The issue is rather the credibility of the person or organization providing the certification, in the eyes of whoever will be relying on that certification.
- IAF-recognized MSS certifications. The best-recognized MSS certifications are those which are made under the umbrella of the International Accreditation Forum. All major countries have an accreditation body which is a member of the IAF, and this body accredits certification bodies in their country to conduct certifications against specific MSSs. (For example, this organization in the UK is called the UK Accreditation Service, or UKAS.) Any certification performed in this way will be recognized world-wide by all other countries

likewise operating in the IAF. Unfortunately, it takes at least a couple of years to kick-start this process. For example, a certification body must already have several certification candidates on which its own certification work can be audited, before the accreditation body will consider giving accreditations.

- Pragmatic approaches. Depending on an organization's own circumstances and requirements, the following might be practical short-term approaches for obtaining meaningful certification against 19770-1:2017.
    - Certification by certification bodies already performing accredited certifications against ISO/IEC 27001. Two examples from the UK are LRQA [Lloyds Register Quality Assurance] and DNVGL [Det Norske Veritas – Global]. These organizations would probably need to subcontract ITAM expertise – especially licensing expertise – from ITAM consulting organizations, but the certification would be that of the certification body, not the ITAM consulting organization. These certifications would probably have the highest level of market recognition possible at present. Note also that there are strong linkages between ITAM and Information Security Management, including the need for a 'Statement of Applicability' for both.
    - Certification by organizations as arranged by specific 'recipient' organizations. This is the approach which has been used for example by the BSA in having accounting firms perform certifications for its Verafirm organizational certification (based on ISO/IEC 19770-1:2012).
    - Certification by ITAM service and consultancy organizations. These could be highly useful and practical especially for internal use, e.g. to identify opportunities for improvement, and to demonstrate good governance over this complex area to the certified organization's management.

6. Why does edition 3 require so much effort to understand?

Several people have commented on the amount of time they have had to spend to (start to) understand edition 3 of the ISO ITAM standard. These are typically people who have previously used edition 2. Why does it require so much effort? Two major explanations seem most relevant:

- **Lack of guidance on how the new standard works.** Edition 3 is just a 'requirements' document, without explanatory information about its structure and about how it works. Additional guidance information is slowly being created (such as this FAQ and some videos), but it isn't sufficient at present. There are two particular aspects of the new standard which need to be understood:
    - **The new way in which ISO Management System Standards (MSSs) work.** Anybody who has worked with other MSSs in the new structure – such as ISO/IEC 27001 or ISO 9001 – will have already encountered this issue, so may not have much trouble with it. But for anyone new to this, it can take some focus and effort. An explanatory paper on ISO Management System Standards is available on the m-assure website, to help with this learning.
    - **The way tiers are implemented in edition 3.** The concept of tiers was introduced in edition 2 (using tables) in response to market feedback which wanted the ability to certify the most critical processes needed for trustworthy data and license compliance, without having to implement and certify every single process. This concept has been retained in edition 3, but it is implemented using a different approach, which is the same approach as is used for ISO/IEC 27001 for Information Security Management. This requires selecting (additional tier 2 and 3) objectives

from Annex A, and then documenting this selection in a 'Statement of Applicability' (as for ISO/IEC 27001).

- **Need to learn a new approach to organizational integration.** The new ISO MSS approach is highly focused on driving the management system from top-level organizational objectives. Likewise, it requires (and 19770-1:2017 emphasizes) the need to coordinate and integrate with other systems such as for information security. The benefits of this new focus on organizational integration should be clear, not just for operational purposes, but in terms of better communication with management and with all areas of the organization. But it takes some focus and effort to understand and apply this approach. It will help us break down the silos. Technology and licensing are not the only things which change for ITAM professionals!

The answer to the first question also helps to answer this question.

7. Why is risk management both in clause 6 and in the optional add-ons for clause 8?

Clause 6.1 discusses risk management in detail (risk assessment, risk treatment, etc.). There is also an optional functional process area called "Other Risk Management" which can be added to clause 8 (from Annex A). What is the difference between the two?

The answer lies in the way all Management System Standards are supposed to be constructed. Clause 6 is for planning, during which you identify risks and determine how you will manage them. Clause 8 is for operation, where you implement much of that planning.

Many/most of the operational processes in clause 8 manage risks identified in 6.1. For example, 'license management' manages license compliance risk. Change management manages the risk of uncontrolled changes. Security management manages security risks. These are all mandatory risk categories to be managed, so they are included in the base requirements of clause 8. However, there are many other categories of risk which may need to be addressed, depending on what management decides in 6.1 to include in the IT asset management system. Many of these are addressed by the optional processes listed in Annex A – such as contract management and service level management. However, it was neither practical nor indeed possible to have individual operational processes for every possible risk to be addressed, so the catch-all process was added of 'other risk management'. Note that its description states 'The objective of the Other risk management process is to manage identified risks which are not covered by any of the other functional process areas.' Examples of the types of risks which could be managed via this process are business continuity risks; environmental impact risks; and legal risks which may be highly jurisdiction-dependent.