ISO ITAM/SAM: ISO/IEC 19770-1 Edition 3

ISO/IEC 19770-1:2017
published December 2017

Presentation version of 4 April 2018

19770

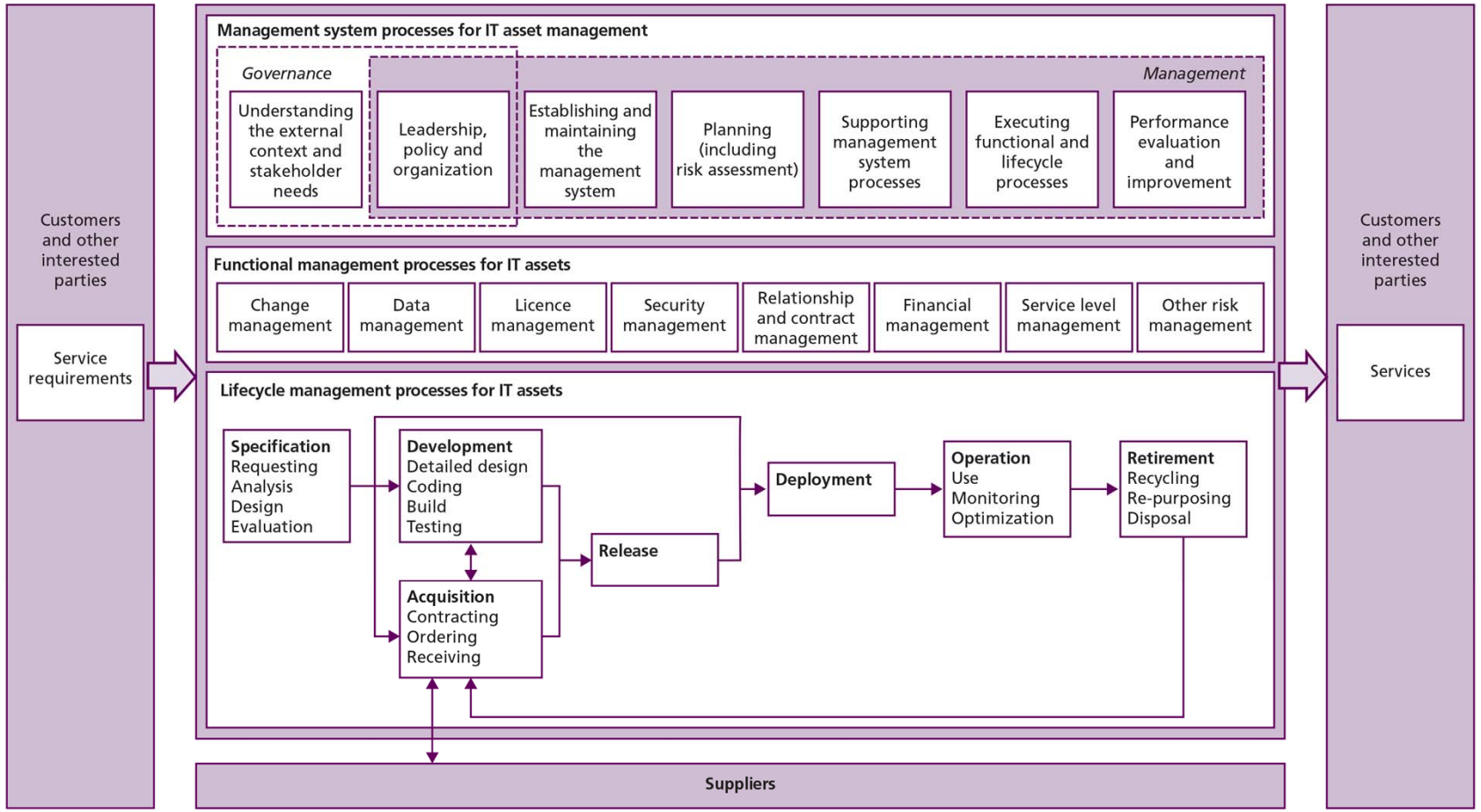
Purpose of Presentation

- To explain edition 3 of 19770-1 to SAM and ITAM professionals, and to other interested individuals, by providing both context and also more detail than is available from the ISO preview (see references at end)
- Context includes
  - Why we want such a standard
  - How it relates to other standards
- The deck, or parts of it, may be used by SAM and ITAM professionals to communicate this information to other interested parties

Contents

- Process standards
- Management system standards
- IT asset management & physical asset management
- ISO ITAM overview
- ISO ITAM contents
- ISO ITAM process objectives & tiers
- Where to obtain
- Additional resources

Overview of 19770-1:2017



What is a Process Standard

- Specification of the processes for a particular functional area
- Most market-significant approach is the ISO Management System Standard
  - ISO 9001 Quality Management
  - ISO/IEC 27001 Information Security Management
  - Many more (see references at end)

Why Have a Process Standard?

- Facilitate common industry terminology and approaches in products and services
  - Facilitate training and awareness
  - Facilitate comparability of suppliers
  - Facilitate organizational assessment against agreed baseline
- Allow independent certification

Management System Standards

- Management System Standards (MSSs) are process standards written in an ISO-specified way
- Both 27001 (Information Security Management – ISM) and 19770-1 (IT Asset Management – ITAM) are Management System Standards (MSSs) using the ISO-mandated 'high level structure and common wording' from 'Annex SL' to ISO directives
- All MSSs (since ca 2013) also comply e.g. 9001 (Quality Management) and 14001 (Environmental Management)
- 20000-1 (IT Service Management) is currently being rewritten in this way
- All look the same at the top level; differences are in the detail, via *additions*

Why Have an MSS ITAM Process Standard

- Alignment with all MSSs
  - Greater understanding by all people working with MSSs
- Specific alignment/integration with
  - Security (ISO/IEC 27001)
  - Service Management (ISO/IEC 20000-1)
- More uptake of the standard
- ISO requirement for our type of standard

MSS Examples

- ISO 9001 Quality Management
- ISO/IEC 27001 Information Security Management
- ISO/IEC 19770-1 Software Asset Management
- ISO/IEC 20000-1 Service Management
- ISO 55001 Asset Management
- ISO 22301 Business Continuity Management
- ISO 14001 Environmental Management
- ISO 20121 Event Sustainability Management
- ISO 22000 Food Safety Management
- ISO 34001 Security Management
- ISO 41000 Facilities Management
- ISO 45001 Occupational Health & Safety Management
- ISO 50001 Energy Management
- … and more

MSS High Level Structure (1)

Introduction

1. **Scope**
2. **Normative references**
3. **Terms and definitions**
4. **Context of the organization**

4.1 Understanding the organization and its context

4.2 Understanding the needs and expectations of interested parties

4.3 Determining the scope of the XXX management system

4.4 XXX management system

5. **Leadership**

5.1 Leadership and commitment

5.2 Policy

5.3 Organizational roles, responsibilities and authorities

Where the text "XXX" appears, the appropriate reference should be inserted depending on the context. For example: "an XXX objective" could be substituted as "an information security objective".

MSS High Level Structure (2)

6. Planning

6.1 Actions to address risks and opportunities

6.2 XXX objectives and planning to achieve them

7. Support

7.1 Resources

7.2 Competence

7.3 Awareness

7.4 Communication

7.5 Documented information

7.5.1 General

7.5.2 Creating and updating

7.5.3 Control of documented information

MSS High Level Structure (3)

8. Operation

8.1 Operational planning and control

9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit

9.3 Management review

10. Improvement

10.1 Nonconformity and corrective action

10.2 Continual improvement

This is the clause where most discipline-specific detail is expected to be added

MSS Issues

- It is a big improvement, but…
- It won't be perfect
  - You can't tell anything about a standard unless you go down into the detail – they all look the same at the top.
  - Some clauses in different standards will have significant differences in the additions.

IT & Physical Asset Management

- ISO ITAM Version 3 written in coordination with ISO 55001:2014 for physical asset management
- 19770-1 is a “discipline-specific extension” of 55001, with changes
  - Both are based on same ISO MSS headings and text
  - 19770-1 is not a “sector-specific application” of 55001
  - Conformance with 19770-1 does not mean conformance with 55001 (although achieving 55001 conformance should be easy)
  - Extensions are especially to deal with software & licensing; also providing for tiers
  - Major change from 55001 is use of risk management approach taken from 27001; all changes detailed in 19770-1 Annex D

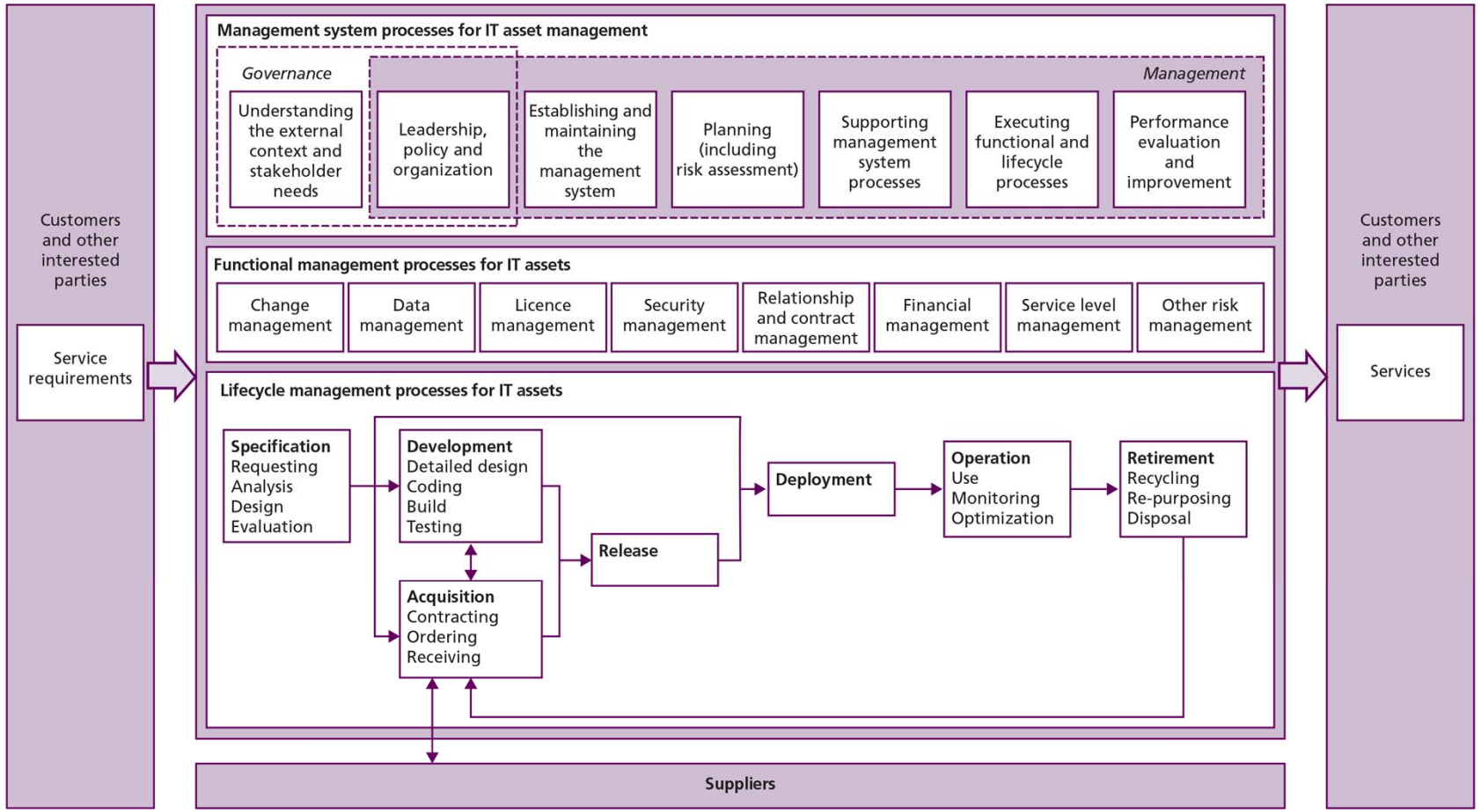
SAM/ITAM Extensions (1)

- Need for extensions because of specific software characteristics
  - Difficulty of controlling
    - Difficulty of controlling modification, duplication and distribution
    - Difficulty of reconciling with other systems
  - Complexity
    - Flexibility of location
    - Number of components
    - Rate of change
    - Versioning of components
  - Licensing
  - Detailed in 19770-1 Annex C

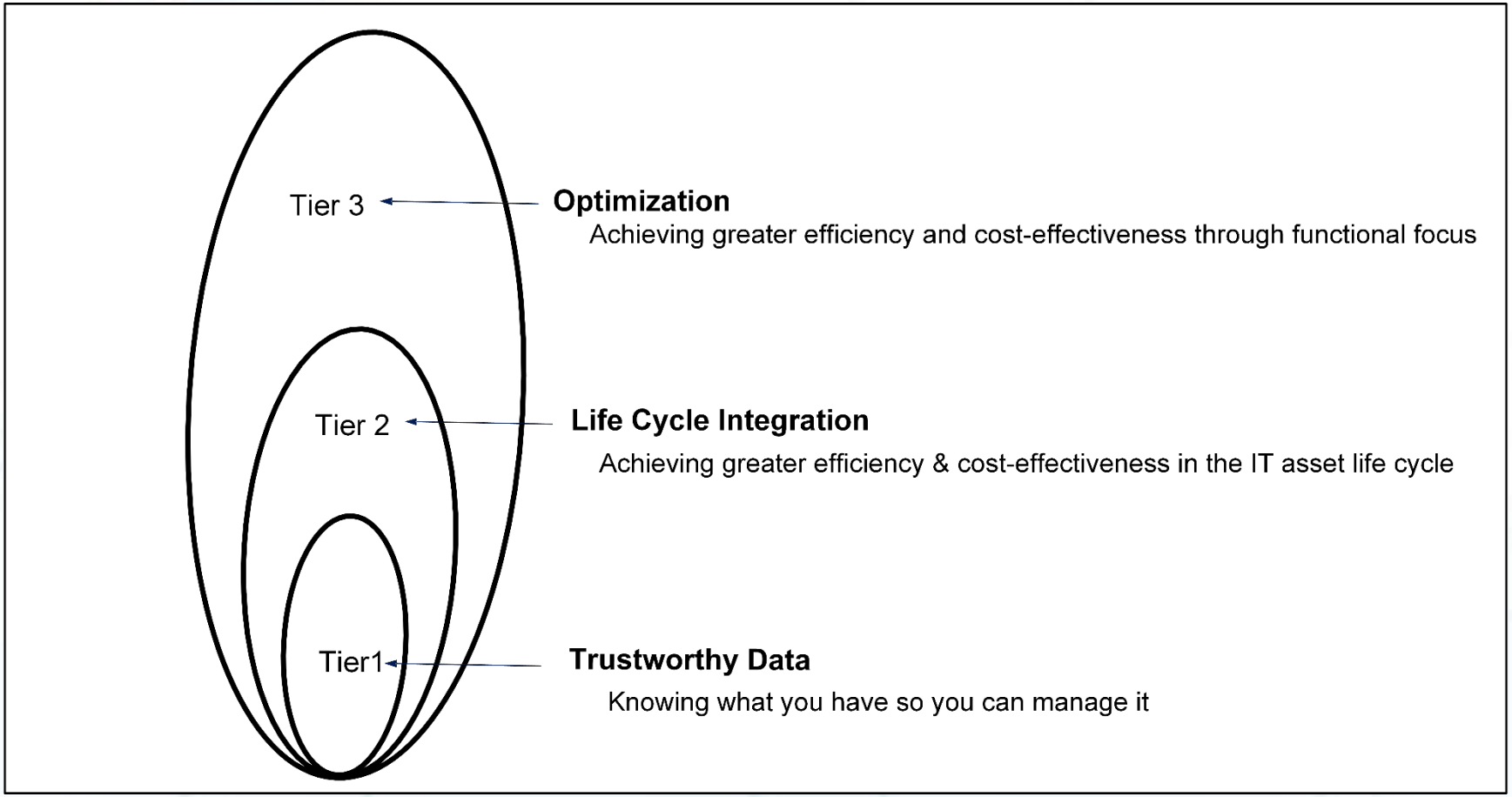
SAM/ITAM Extensions (2)

- Nature of extensions
  - Controls over software modification, duplication and distribution, with particular emphasis on access and integrity controls
  - Audit trails of authorizations and of changes made to IT assets
  - Controls over licensing, underlicensing, overlicensing, and compliance with licensing terms and conditions
  - Controls over situations involving mixed ownership and responsibilities, such as in cloud computing and with ‘Bring-Your-Own-Device’ (BYOD) practices
  - Reconciliation of IT asset management data with data in other information systems when justified by business value, in particular with financial information systems recording assets and expenses
  - See also 19770-1 Introduction

Overview of 19770-1:2017



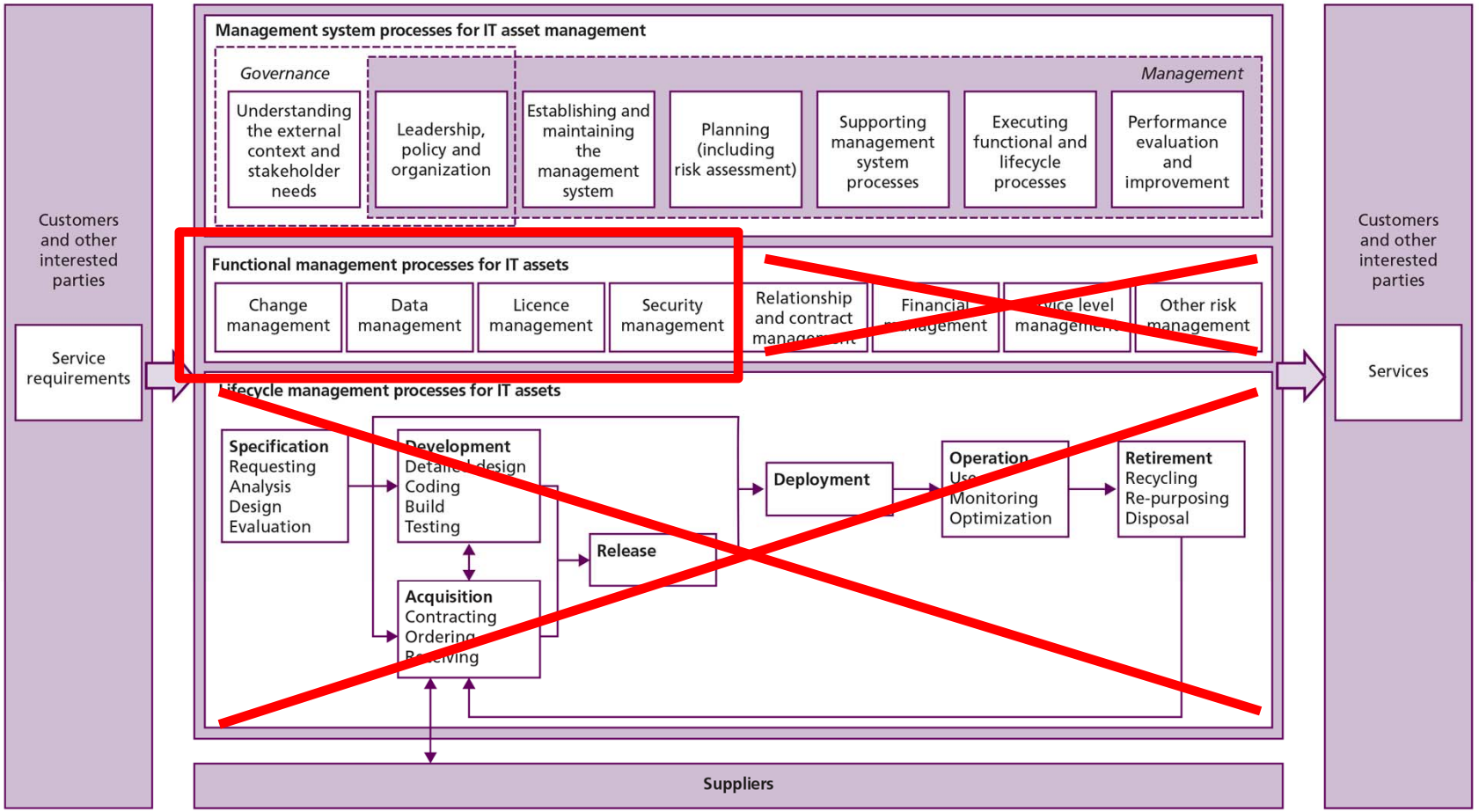
Tiers (1)



Tiers (2)

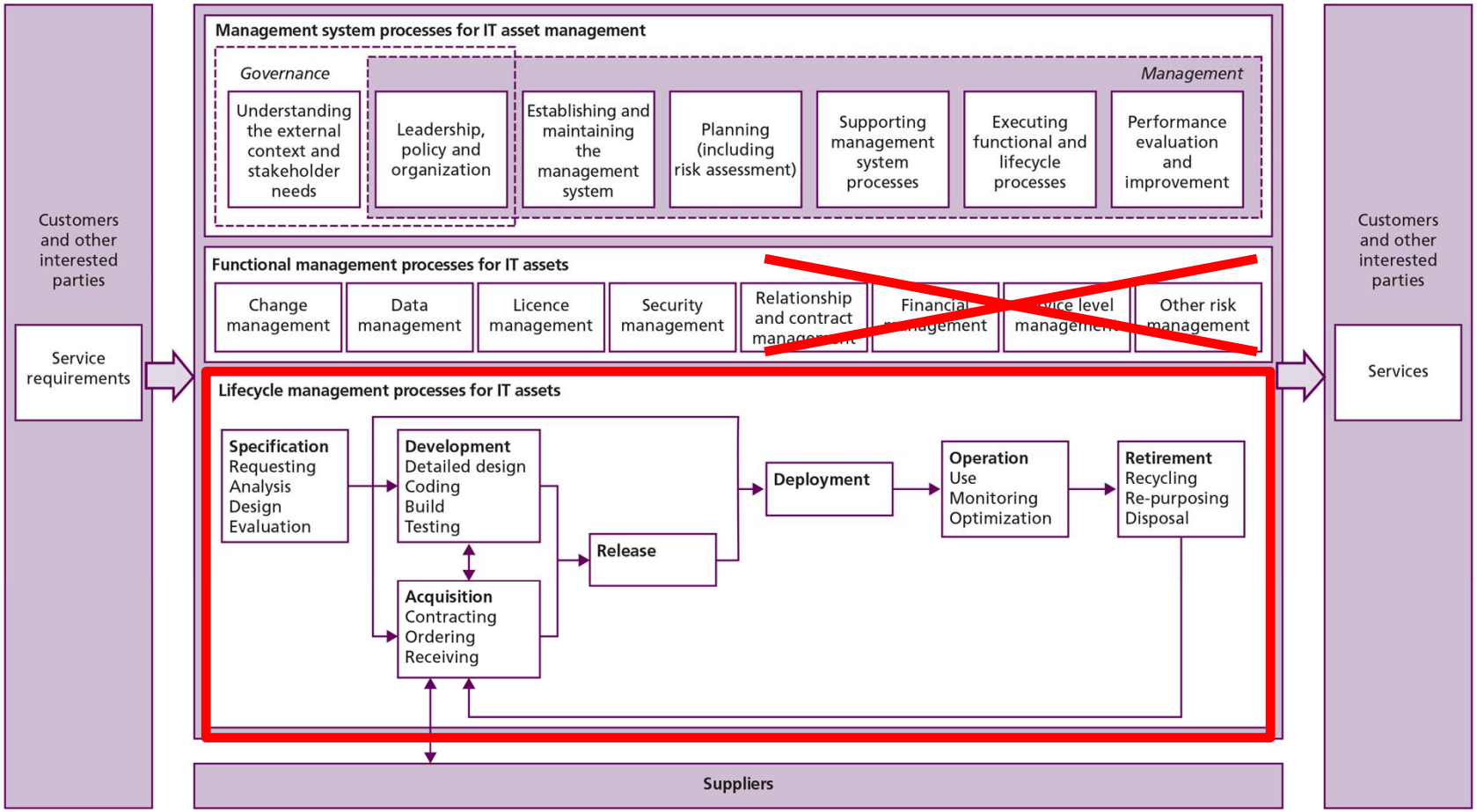
- Tiers are additional to “Management System Processes for IT Asset Management”
- Tiers are suggested groupings of operational objectives from Annex A
  - Use of these names and groupings is optional but highly recommended
- Tier 1 objectives are already included in main body of standard and are mandatory
  - Called “Trustworthy Data”
  - Includes Change Management, Data Management, License Management, and Security Management
- Tier 2 & 3 groupings of objectives are additional and optional
  - Intended to be cumulative

Tier 1 - Required

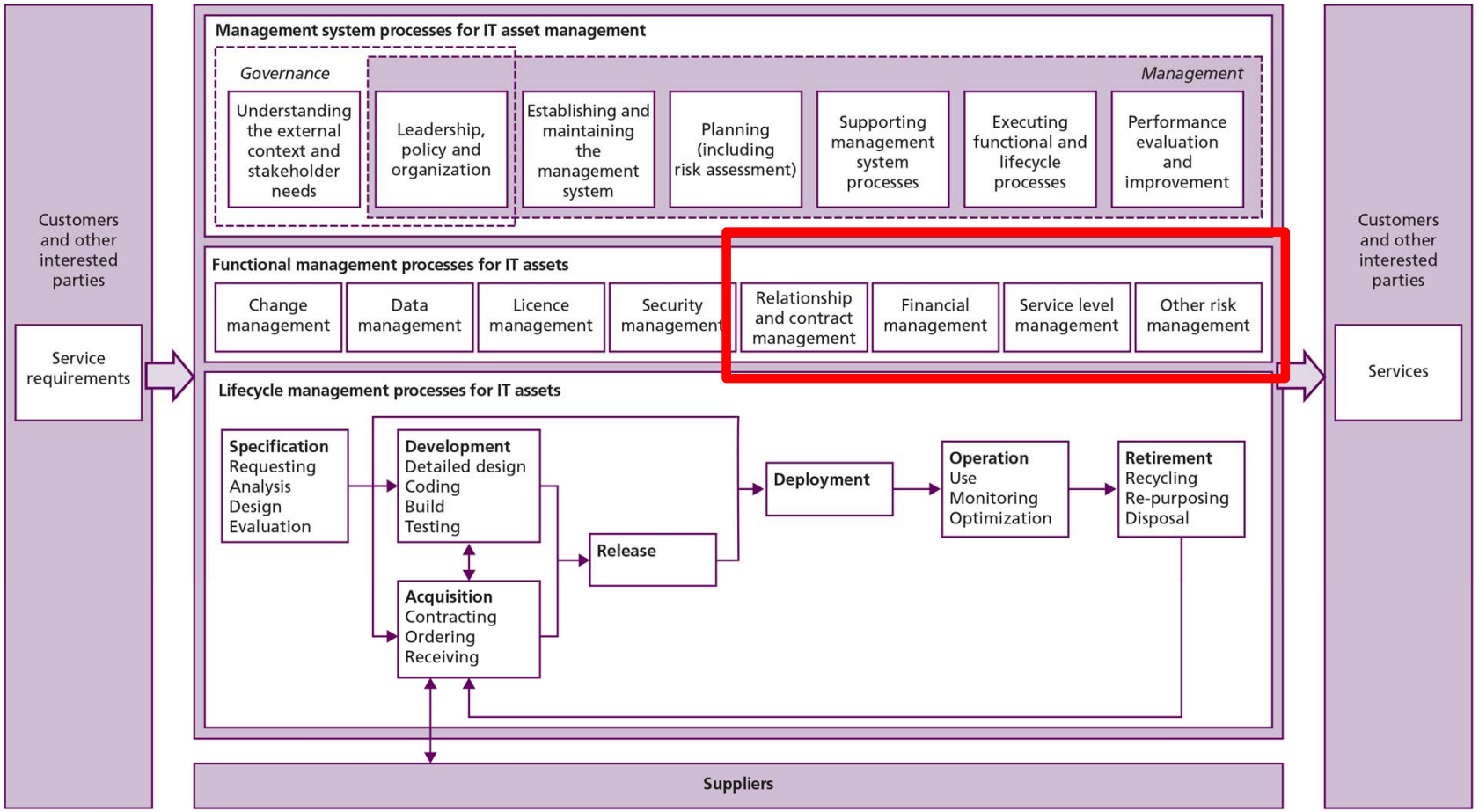


Reproduced with kind permission from The Stationery Office, ITIL Guide to Software and IT Asset Management, Bicket and Rudd, 2018. ISBN 9780113315482

Tier 2 - Optional



Tier 3 - Optional



19770-1 Ed 3 Contents (1)

Headings/content in black are required by ISO

Headings/content in green were added by 55001

Headings/content in red were added by 19770-1

19770-1 Ed 3 Contents (2)

19770-1 Ed 3 Contents (3)

19770-1 Ed 3 Contents (4)

8 Operation

8.1 Operational planning and control

8.2 Management of change

8.3 Core data management

8.4 License management

8.5 Security management

Tier 1

8.6 Other processes

For adding other processes especially Tiers 2 & 3

8.7 Outsourcing and services

8.8 Mixed responsibilities between the organization and its personnel

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit

9.3 Management review

19770-1 Ed 3 Contents (5)

Organizational Certification

- Editions 1 & 2
  - Different approach to most other standards (and more difficult) because of SC7 requirements for WG21 at time of writing
  - See references for details on organizations certified
- Edition 3 (MSS)
  - All MSS auditors will be capable of certifying (especially organizations which certify against 27001)
  - But need to have appropriate subject-matter expertise
    - Can be contracted in from SAM/ITAM specialist organizations

How to Get Involved

- Formally, through ISO national bodies
  - ANSI for US – contact ustg21convenor@19770.org
  - BSI for UK
  - DIN for Germany
  - AFNOR for France
  - Etc
- Potentially via liaison bodies
  - IAITAM
  - SAMAC (Japan)
  - TagVault
  - Etc

Where to Obtain

- ISO (https://www.iso.org/standard/68531.html) CHF 158
- ANSI (https://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2FIEC%2019770-1:2017&sourcekeyword=&source=google&adgroup=iso13&gclid=EAIaIQobChMI46qGkuTZ2AIVDGcbCh0agwqTEAAYASAAEgLVUPD_BwE) $185
- BSI (https://shop.bsigroup.com/ProductDetail/?pid=000000000030326001) £224 (members £112)
- Other national standards bodies and commercial sources

Additional Resources

- ISO free preview of 19770-1 including all terms and definitions (https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-1:ed-3:v1:en)
- ISO ITAM/SAM overview and terminology: freely available standard (http://standards.iso.org/iso/19770/-5/)
- en.wikipedia.org/wiki/ISO/IEC_19770
- m-assure.com/blog-links
  - ISO SAM certifications
  - Unique characteristics of IT assets
- download a comprehensive list of 78 Management System Standards from www.iso.org/management-system-standards-list.html

Additional Resources

See also www.m-assure.com for additional resources about ISO ITAM which include:

- FAQs
- Management System Standards – a tutorial for SAM and ITAM practitioners
- This presentation and the video
- A presentation and video on implementing ISO ITAM and ISO information security management together
- Links to the ITIL SAM/ITAM Guide, which also includes information about ISO ITAM