INTERNATIONAL STANDARD

ISO/IEC 27034-5

First edition
2017-10

Information technology — Security techniques — Application security —

Part 5: Protocols and application security controls data structure

Technologies de l'information — Techniques de securite — Securite des applications —

Partie 5: Protocoles et structure de données de contrôles de sécurité d'application

Reference number
ISO/IEC 27034-5:2017(E)

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

Contents

Page

Foreword

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

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

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

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

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

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

A list of all parts in the ISO/IEC 27034 series can be found on the ISO website.

Introduction

General

There is an increasing need for organizations to focus on protecting their information at the application level. A systematic approach towards increasing the level of application security provides an organization with evidence that information being used or stored by its applications is being adequately protected.

ISO/IEC 27034 (all parts) provides concepts, principles, frameworks, components and processes to assist organizations in integrating security seamlessly throughout the life cycle of their applications.

The Application Security Control (ASC) is one of the key components of this document.

To facilitate the implementation of ISO/IEC 27034 (all parts) application security framework and the communication and exchange of ASCs, a minimal set of essential attributes should be documented and explained for realizing ASCs and certain other components of the framework.

This document explains the minimal set of essential attributes of ASCs and further details the Application Security Life Cycle Reference Model (ASLCRM).

Purpose

The purpose of this document is to document and explain the essential information and data structure requirements for ASCs. The advantages of a standardized set of essential information attributes and data structure of ASCs include the following:

a) normalized ASC creation, communication, protection and verification in compliance with the requirements of this document; and

b) minimized cost of security in application projects by facilitating the reuse of approved controls and acquisition of ASCs from different sources."

In addition, this document defines and details the processes, activities and roles involved in the Application Security Life Cycle Reference Model.

Targeted audiences

General

The following audiences will find values and benefits when carrying their designated organizational roles:

a) managers;

b) ONF committee;

c) domain experts;

d) suppliers; and

e) acquirers.

Managers

Managers should read this document because they are responsible for:

a) ensuring the ASCs are reusable within the organization, and

b) ensuring the ASCs are available, communicated and used in application projects with proper tools and procedures all across the organization.

Organization Normative Framework (ONF) Committee

The ONF Committee is responsible for managing the implementation and maintenance of the application-security-related components and processes in the Organization Normative Framework. The ONF Committee:

a) implements the ASC Library,

b) approves ASCs that correctly mitigate application security risks, and

c) manages the cost of implementing and maintaining the ASCs.

Domain experts

Domain experts contribute knowledge in application provisioning, operating or auditing, who:

a) participate in ASC development, validation and verification,

b) participate in ASC implementation and maintenance, by proposing strategies, components and implementation processes for adapting ASCs to the organization's context, and

c) validate that ASCs are useable and useful in application projects.

Security tools and ASC supplier

Suppliers contribute to develop, maintain and distribute tools and/or ASCs. They

a) create, validate, enforce integrity (through a recognized method, such as signing), distribute and apply ASCs, and

b) align with a common and standardized exchange protocol (structure and format) for ASCs.

Security tools and ASC acquirer

Acquires are individuals or organizations who want to acquire ASCs. They

a) integrate ASCs into their organization and ensure the interoperability of any internal and third-party ASCs,

b) adapt ASCs and enforce their integrity, and

c) ensure that the activities and tasks of acquired ASCs can be mapped to the organization's application lifecycle.

Information technology — Security techniques — Application security —

Part 5: Protocols and application security controls data structure

1 Scope

This document outlines and explains the minimal set of essential attributes of ASCs and details the activities and roles of the Application Security Life Cycle Reference Model (ASLCRM).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27034-1, *Information technology — Security techniques — Application security — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27034-1 and the following apply.

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

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

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

3.1
activity
set of actions or tasks carried out by an actor during the application's life cycle

3.2
information group record
list of information elements to which an organization can assign labels, such as names, description and categorization values

Note 1 to entry: To avoid confusion, information group name should be unique within the organization.

3.3
information element
piece of information that should be categorized and identified by a name, description, and domain values (e.g. a field in a database)

Note 1 to entry: An information group can be seen as an information element.

4 Abbreviated terms

ASC	Application Security Control
ASLC	Application Security Life Cycle
ASLCRM	Application Security Life Cycle Reference Model
ICT	Information and Communication Technology
ONF	Organization Normative Framework

5 Application Security Control Structure

5.1 General

Each Application Security Control (ASC) defines a security-related activity performed at a specific point in an application's life cycle to mitigate a risk or to satisfy a requirement. The security activity is supplemented by a verification measurement (activity) that specifies the necessary steps to verify its successful application. For both the security activity and verification measurement, an ASC specifies how, where, when and by whom the activity should be implemented. Information about the required effort is also captured.

The purpose of this clause is to provide a specification of the ASC information requirements and data structure recommendations. Organizations may choose to implement the information requirements and data structure requirements using either a narrative approach or other suitable data structure, which best suits organizational needs and requirements.

NOTE 1 To identifiy the minimum set of attributes needed to define a valid ASC, the name of each ASC attribute defined in this document includes the mention "**(M)**" when the attribute is **mandatory**, or the mention "**(O)**" when the attribute is **optional**.

NOTE 2 The inclusion of an optional attribute could require the implementation of subsequent mandatory attributes. Mandatory attributes under an optional attribute are mandatory only when the optional attribute is implemented [e.g. see 5.2.4.2, e)].

The purpose of this clause is also to provide a list of possible activities enabling the ONF Committee to attach ASCs into the Application Security Life Cycle Reference Model (ASLCRM).

ASC developers should align their vocabulary with ISO/IEC 27034 (all parts) when they need to describe assets.

5.2 ASC information requirements

5.2.1 Overview

This subclause defines the recommended information requirements for individual application security controls. For a concrete implementation in form of an XML Schema of this document, please refer to ISO/IEC 27034-5-1.

Note that this document does not define how the various ASC information items are identified or managed. For details about the latter, consult the management and audit process defined in ISO/IEC 27034-2, ISO/IEC 27034-3 and ISO/IEC 27034-4.

NOTE Explicit indication of an inheritance hierarchy is not implemented in the ASC structure, but could be implemented in future versions.

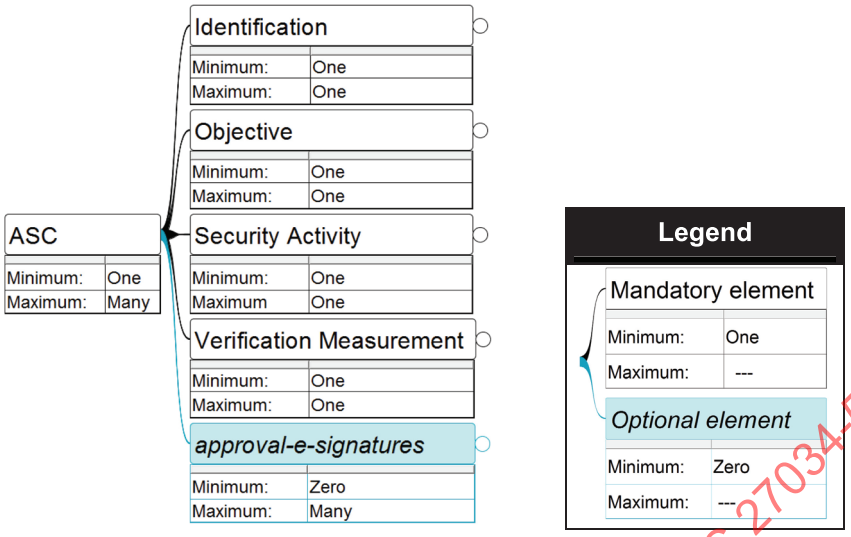

Figure 1 — Main sections of ASC information

As specified in ISO/IEC 27034-1:2011, 8.1.2.6.5, and shown in Figure 1, each ASC should contain the following sections:

a) **ASC Identification (M):** This section should contain the following information:

   1) identification information about the ASC (id, name, etc.);

   2) a high-level description of the scope and intent of the ASC;

   3) information about the current version including the creation date, current lifecycle stage, revision notes and identification information about its author and owner; and

   4) references to super-ordinate and sub-ordinate ASCs.

b) **ASC Objective (M):** This section should contain the following information:

   1) a detailed description of the ASC's intent and security objective;

   2) one or more security requirements that justify 'why' the ASC is needed as well as information about the context and the application functionality from which the security requirements originated;

   3) one or more levels of trust for which the ASC is mandatory along with a description of the level of trust range;

   4) preconditions and assumptions for applying the ASC. In particular:

      i) a list of preconditions;

      ii) a list of (informal) threat assumptions; and

      iii) a description of the operating environment (context of use).

c) **ASC Security Activity (M):** This section should contain the following information pertinent to the security activity defined by the ASC:

   1) a high-level description of the security activity (what);

   2) a description of the asset that is protected (targeted) by carrying out the security activity (where);

3) a definition of the roles (and required qualifications) involved in the execution of the tasks and actions involved in the security activity (who);

4) an indication of the complexity and costs of the security activity (how much);

5) a detailed specification of the tasks and actions to be performed by the security activity, the expected outcomes and preconditions (how); and

6) an indication as to when (relative to Application Security Life Cycle Reference Model) the tasks and actions of the security activity should be performed (when).

d) **ASC Verification Measurement (M):** This section should contain the following information pertinent to the verification measurements defined by the ASC:

1) a high-level description of the verification measurement (what);

2) a description of the asset that is verified (audited) by the verification measurement (where);

3) a definition of the roles (and required qualifications) involved in the execution of the tasks and actions involved in the verification activity (who);

4) an indication of the complexity and costs of the verification measurement (how much);

5) a detailed specification of the tasks and actions to be performed by the verification activity, the expected outcomes and preconditions (how); and

6) an indication as to when (relative to Application Security Life Cycle Reference Model) the tasks and actions of the verification activity should be performed (when).

Further details for each information requirement are provided in 5.2.4.

5.2.2 Integrity assurance

In order to ensure the integrity of contents of ASCs, an ASC should be 'signable' (or similar recognized method). It should support cascading and multiple e-signatures as well as timestamps.

5.2.3 Multilingual/multiregional data representation

In order to ensure global communication of ASCs, the ASC data structure should support localized text and the specification of information items, processes or ICT in multiple languages.

5.2.4 ASC information requirements

5.2.4.1 Identification (M)

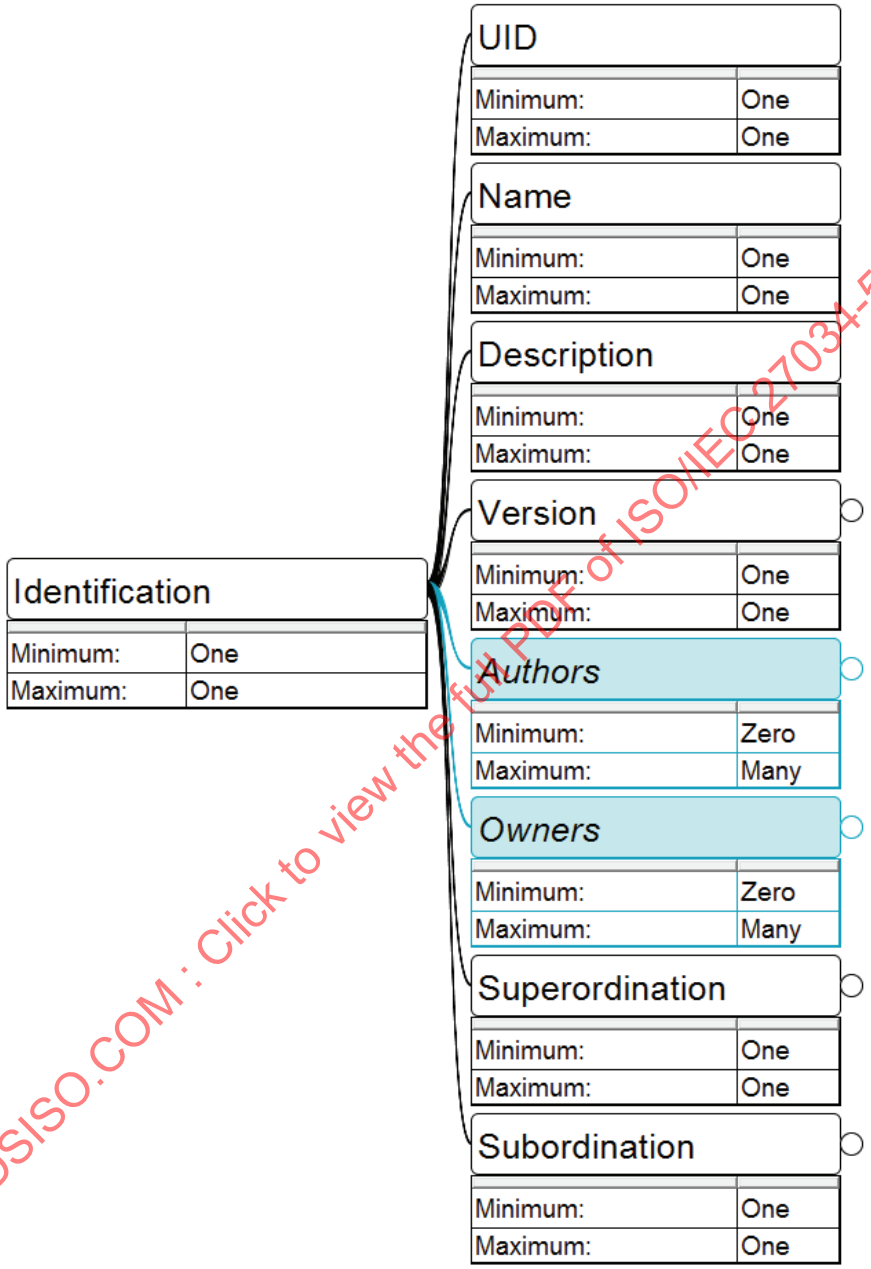

Figure 2 — Identification section of an ASC

As shown in Figure 2, an ASC should contain the following information pertinent to its identity:

a) Identification information about the ASC including:

   1) **UID (M):** A unique identifier inside the schema;

   2) **Name (M):** A representative name;

b) **Description (M):** High-level description of the ASCs intent and scope;

c) **Version (M):** Information describing this ASC version, including:

1) **Number (M):** The current version number of the ASC, using legal style numbering (e.g. 0.1.1 or 1.2);

2) **Date (M):** The creation date of the current version of the ASC;

3) **Life cycle stage (M):** The currently active stage within the ASC life cycle. The following life cycle stage values are permissible:

i) creation request;

ii) design;

iii) design review and validation;

iv) development;

v) verification;

vi) approval;

vii) owners final approval;

viii) published for training;

ix) active;

x) expired;

xi) custom.

4) **Maturity approval note (O):** A maturity level indication of this version;

5) **Revision notes (O):** A description of *how* the ASC evolved from the previous version;

d) **Author (O):** Authors of the current version of the ASC and its affiliation, including their names and contact information; and

e) **Owner (O):** Owners of the current version of the ASC and its affiliation, including their names and contact information.

f) Graph relationships to super-ordinate and sub-ordinate ASCs are defined as follows and as illustrated in Figure 3:

1) **Subordination (M):** References to zero, one or many subordinated ASCs' unique identification numbers as a way to specify that the completion of the activities of all subordinate (children) ASCs (in the order defined) is necessary to complete the activity of the superordinate ASC. A short description of refered ASCs may be included.

2) **Superordination (M):** Reference to zero, one or many superordinate ASCs' unique identification numbers as a way to specify its parent ASCs. A short description of refered parent ASCs may be included.

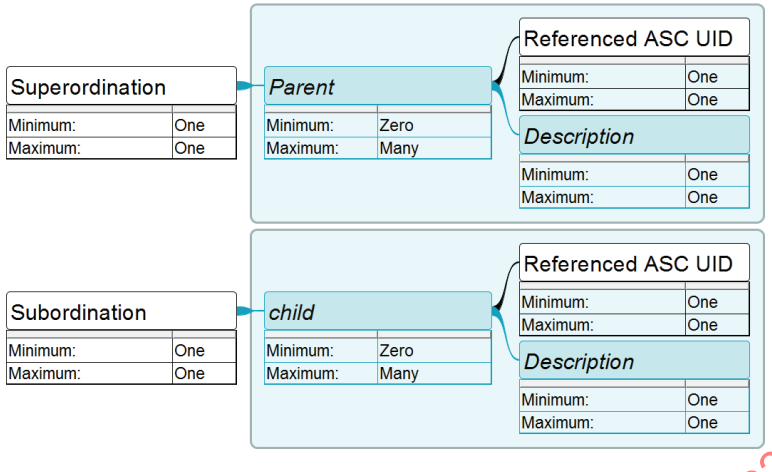

Figure 3 — ASC graph relationship

5.2.4.2 Objectives

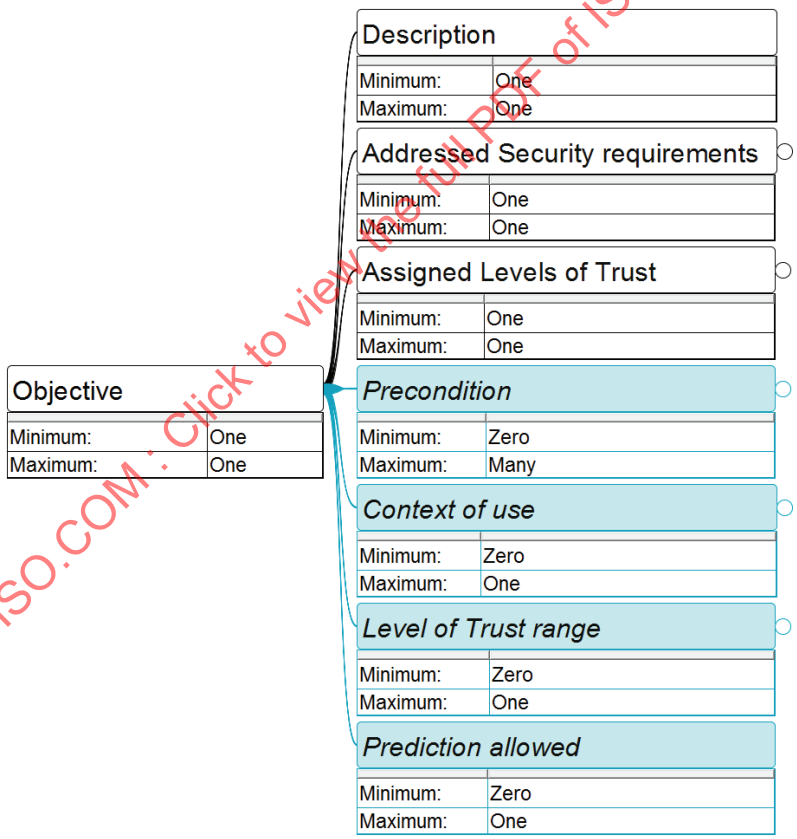

Figure 4 — Objective section of an ASC

As shown in Figure 4, an ASC should contain the following information pertinent to its security objectives:

a) **Description (M):** A detailed description of the ASC's purpose and security objectives;

b) **Addressed Security requirements (M):** A non-empty set of requirements that are addressed by performing the security activity of the ASC. For each requirement, the following information should be captured:

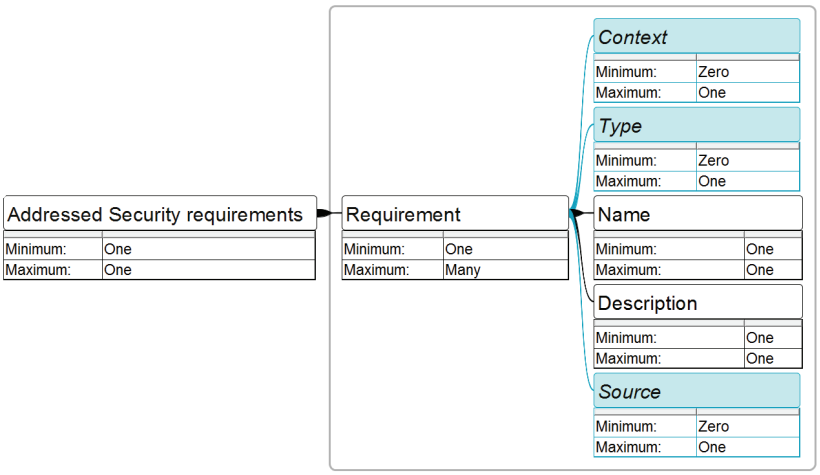

Figure 5 — Security requirement section of an ASC

1) **Context (O):** Specifies the context (source) the requirement originates from. The following context type values are permissible:

   i) regulatory context;

   ii) business context;

   iii) technological context;

   iv) application functionality;

   v) custom.

2) **Type (O):** The type of the security requirements. The following values are permissible:

   i) business requirements;

   ii) business rules;

   iii) regulatory requirements;

   iv) user requirements;

   v) actor qualifications requirements;

   vi) quality attributes;

   vii) system requirements;

   viii) process requirements;

   ix) functional requirements;

   x) external interfaces;

   xi) infrastructure requirements;

   xii) constraints;

   xiii) custom.

3) **Name (M):** A representative name for the requirement;

4) **Description (M):** A qualitative description of the requirement;

5) **Source (O):** The source document from which the requirement originates.

c) **Assigned Levels of Trust (M):** A list of one or more levels of trust for which the ASC is mandatory. In order to keep the ASC self-contained, this information should be complemented by the level of trust range which provides a definition of the assigned levels of trust as well as an indicator of the relative strengths of each level;

d) **Condition (O):** Description of preconditions, assumptions and context of use for applying the ASC, including, as shown in Figure 6:

1) **Condition type (O):** The type of the condition. The following values are permissible:

i) precondition;

ii) assumption;

iii) operating environment description;

iv) custom.

2) **Description (M):** May include the following:

i) a list of preconditions for applying the ASC;

ii) a list of (informal) threat assumptions which are mitigated by the ASC;

iii) a description of the operating environment (context of use).

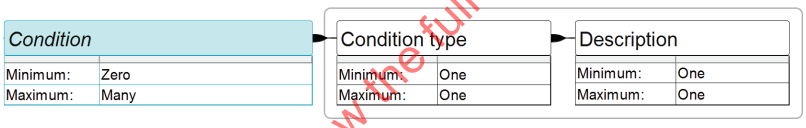

Figure 6 — Condition section of an ASC

e) **Level of Trust range (O)**:

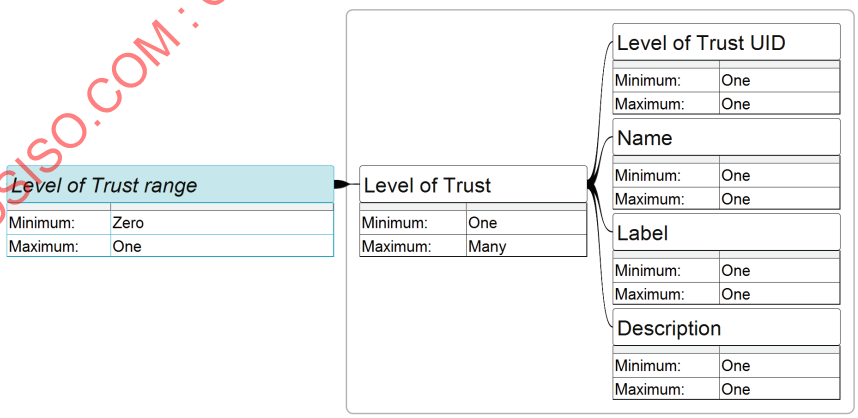

Figure 7 — Level of Trust range section of an ASC

When a Level of Trust range exists in an ASC, the following information, as shown in Figure 7, should describe each Level of Trust included in the range:

1) **Level of Trust UID (M):** Unique identification number in this schema, for this Level of Trust

2) **Name (M):** The Level of Trust name;

3) **Label (M):** A label, representing this Level of Trust;

4) **Description (M):** A short description of the Level of Trust to help the acquirer/receiver to integrate this ASC at the right level in the acquirer's ASC Library.

f) **Prediction allowed indicator (O):** Specifies whether prediction is allowed for the ASC. That is, whether or not the correct functioning of the ASC shall be re-validated or not if the operating context changes in a non-substantial manner. See ISO/IEC 27034-7 for details.

5.2.4.3 Security activity and verification measurement

An ASC should specify one security activity and one associated verification measurement. The security activity specifies a set of tasks and actions that need to be carried out in order to fulfill the security requirements associated with the ASC. The verification measurement specifies the tasks and actions that need to be carried out in order to verify that the security requirements of the ASC have been met.

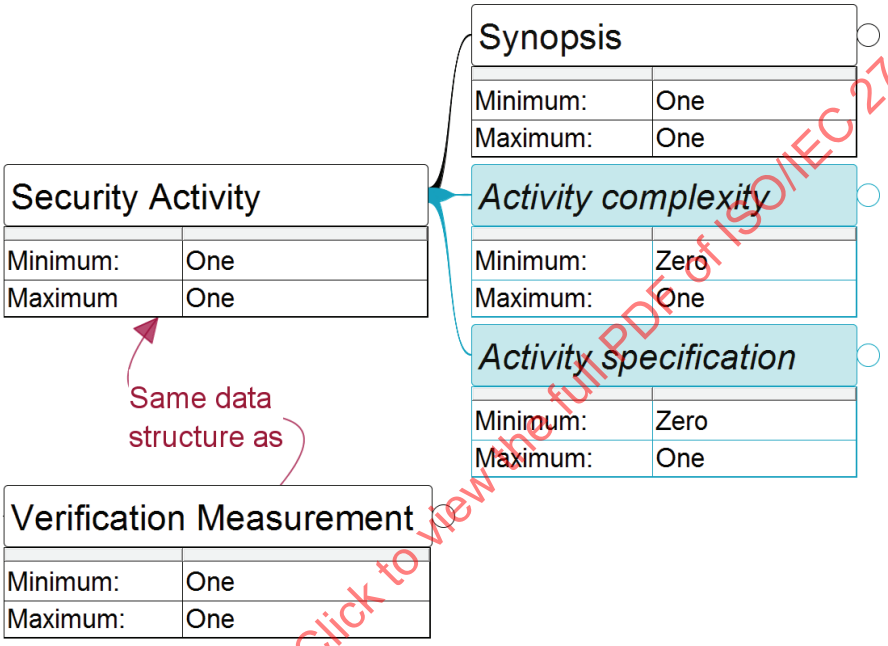

Figure 8 — Security activity and verification measurement sections of an ASC

As shown in Figure 8, an ASC should contain the following information for specifying both the security activity and the verification measurement activity.

a) **Synopsis (M):** A condensed statement giving a general view of this activity. The following information should be captured:

1) **Name (M):** Name of the activity;

2) **Description (M):** An informal description of the scope of the activity including its coverage and outcome;

3) **Target information (M):** An indicator of the scope of the activity. It defines which group of information items are protected / verified by the activity as a result of implementing the ASC to people, processes or information and communications technology (ICT) involved with those information items. In order for an ASC activity to be valid and 'useful' there shall be at least one information item that is protected or verified by the ASC. For each information item the following information is specified:

i) **Name (M):** A representative name for the information item, processes or ICT;

ii) **Information group type (M):** Associates one or more types with the information item, processes or ICT. The following values are permissible:

I) laws and regulations;

II) organization or business line directives and regulations;

III) application life cycle processes;

IV) application process definition;

V) specification;

VI) application data;

VII) organization and user data;

VIII) roles permission definition;

IX) technological context definition;

X) custom.

iii) **Description (M):** A description of the information item, processes or ICT;

iv) **Information classification (O):** An indication of how sensitive (in terms of confidentiality, integrity and availability) the information item is.

v) **Information owner (O):** Identifies the owner of this information item.

4) **Outcome description (M):** A description of the expected outcome as a result of applying the activity.

5) **Supporting expert resources (O):** References to supporting (expert) resources to facilitate the application of the activity.

b) **Activity complexity (O):** Indication of the complexity of the activity using quantitative and qualitative measures.

NOTE This **Activity complexity** attribute is mandatory (M) when the **Activity specification** attribute exists.

c) The following information should be captured:

1) **Label (M):** A descriptive complexity label. The following complexity values are permissible:

i) low;

ii) medium;

iii) high;

iv) extreme;

v) custom.

2) **Description (M)**: A description of the complexity;

3) **Global estimated cost (O):** The estimated (monetary) cost for performing the activity;

4) **Global estimated effort (O):** The effort required to perform the activity (e.g. day/person);

5) **Global estimated time (O):** The time required to complete the activity.

6) **Note (O):** Supplemental information about the complexity of this activity.

d) **Activity specification (O):** A detailed description of the activity.

NOTE This **Activity specification** attribute is optional (O) because it is not required when the ASC is a "head ASC" in an ASC hierarchy (see ISO/IEC 27034-1:2011, Figure 7) (see Figure 3). Otherwise, it is required.

Each activity specification includes a **Responsibility matrix referred (M)** attribute that identifies the type of responsibility matrix referred in this activity description. The following values are permissible:

1) RACI;

2) RASCI.

The following labels are permissible for describing responsibilities:

1) responsible;

2) accountable;

3) support;

4) consulted;

5) informed.

Each activity specification includes a sequence of ordered **tasks (M)**. Each task should contain the following information:

1) **Sequence (O):** Execution sequence number ordering the tasks of this activity.

2) **Description (M):** A description of the task;

3) **Pre-conditions (O):** A set of preconditions (including precedence requirements) that need to be satisfied before the task can be performed;

4) **Required resources (M):** The resources involved (and required) for performing the task. For each resource allocation, the following information is specified:

   i) **Role name (M):** A reference to the role that will be fulfilled by the resource. The set of possible roles is defined by the ASLCRM (see 6.6).

   ii) **Responsibility (M)**: The RACI responsibility assumed by the role for that task.

   iii) **Description (O)**: A description of the nature of the resource allocation; and

   iv) **Required qualifications (O):** A list of qualifications required to assume the role's responsibility in the execution of the tasks and actions of the activity. For each role, the qualifications required should be specified.

5) **Execution moments (M):** Indication of when [relative to the activities defined in the Application Security Lifecycle Reference Model (Clause 6)] the task shall be performed. For each execution moment the following information should be specified:

   i) **Execution order (M):** The execution order relative to the referenced activity. The following values are permissible:

      I) before;

      II) during;

      III) after;

IV) custom.

ii) **Life cycle reference (M):** A reference to an activity in the Application Security Lifecycle Reference. The values permissible for the role are defined by the ASRLCM (Clause 6);

iii) **Name (O):** An activity name, when the activity is referencing "Custom" in the life-cycle-reference.

iv) **Description (M):** A description of when the task shall be performed;

v) **Interval value, unit and label (M):** The execution frequency value of the task.

I) The following time units are permissible for describing an interval value:

A) seconds;

B) minutes;

C) hours;

D) days;

E) weeks;

F) months;

G) semesters;

H) years.

II) The following labels are permissible for describing an interval:

A) once;

B) periodic;

C) on event;

D) custom.

6) **Actions list (M):** A sequence of low-level atomic action descriptions that need to be executed in order to complete the task;

7) **Outcome (M):** The expected outcome of the task in terms of which artefacts are expected to be produced as a result of task performance. For each expected artefact, the following information should be specified:

i) **Type (M):** The type of artefact produced. The following values are permissible:

I) report;

II) document;

III) source code;

IV) compiled code;

V) executable code;

VI) script;

VII) library;

VIII) diagram;

IX) parameters file;

X) link;

XI) custom.

ii) **Content (M):** The expected content of the produced artefact.

8) **Task estimated effort (O)**: The estimated effort required by the resource allocation to complete this task.

9) **Note (O):** Provides additional information about this task if needed.

5.2.4.4 Self-containedness recommendation

When importing ASCs, a self-contained set of ASCs should be imported, i.e. all ASCs linked through a hierarchy should be imported together.

Similarly references between ASCs acquired from an ASC supplier should be mapped to the referencing scheme of the acquirer's own ASC Library.

5.3 ASC data structure recommendations

5.3.1 General

In what follows a set of recommendations is made for defining a suitable data structure for ASCs. The objective of these recommendations is to facilitate exchange and communication of ASCs while preserving their integrity.

5.3.2 Exchange

In order to foster the broad adoption and sharing of ASCs, an ASC should be defined in a platform-independent and portable manner. ASCs should be communicated using the notation described in ISO/IEC 27034-5-1.

5.3.3 Self-containedness

In order to ensure that ASCs can be understood and applied without consulting external documents, the ASC data structure should support the inclusion of complex (non-text) data elements, such as documents, source or executable code, etc. It is highly recommended *to include the range of levels of trust* based on which recommended levels of trust the ASC has been defined for.

The identification and description of an item in an ASC should be understandable without a context, if standardized identification schemes are used. E.g. ISO/IEC 19770-5 and ISO/IEC 19770-2.

6 Application Security Life Cycle Reference Model

6.1 General

The purpose of this clause is to further detail and list the activity labels proposed by the Application Security Life Cycle Reference Model (ASLCRM) defined in ISO/IEC 27034-1. Figure 9 shows that the life cycle of an application consists basically of two stages: Provisioning and Operation. The former is further broken down into Preparation, Realization and Transition phases while the latter is subdivided into Utilization / Maintenance, Archival and Destruction phases. In each phase, a set of activities in application management, application provisioning and operation, infrastructure management and application audit are executed involving several actors. It is the purpose of 6.2 to 6.6 to further detail these activity labels as well as to provide generic definitions of the actors involved.

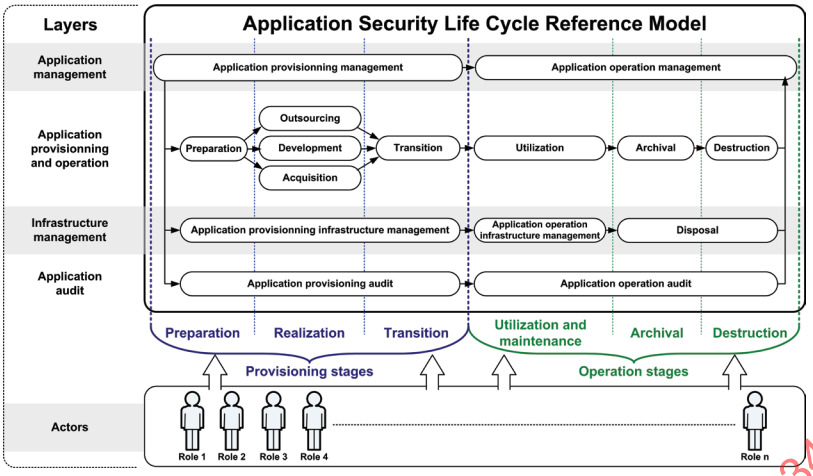

Figure 9 — Top-level view of the Application Security Life Cycle Reference Model

The various stages, phases and activities defined by the ASLCRM should be used as a referential in the ASC definition to indicate when an ASC activity should be performed. Similarly, the actors and roles defined by the ASLCRM should be used as referential in the ASC definition to indicate which resources should be allocated for performing an ASC activity or task.

Figure 10 presents the ASLCRM elements as a tree, where the root is the "Life cycle reference" element, the first level is the "layer", the second level is the "stage", the third level is the "activity area", the fourth level is the "activity sub-area" and the fifth level is the "activity label" itself. A path, as a sequence of elements, may be selected to identify one specific activity label as an execution moment (5.2.4.3, d)5)).

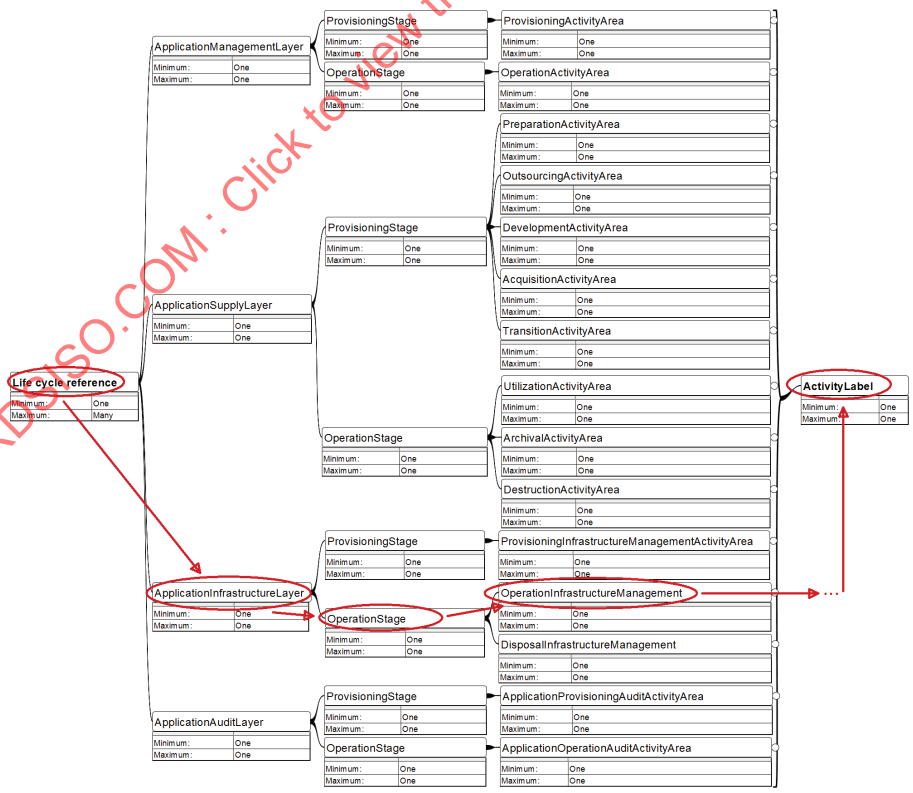

Figure 10 — ActivityLabel selected from the Application Security Life Cycle Reference Model

In this example, the complete sequence to identify the activity label is: "Life Cycle Reference / Application Infrastructure Layer / Operation Stage / Operation Infrastructure Management / … /Activity Label".

6.2 Application Management Layer

6.2.1 General

Figure 11 — Application Management Processes

NOTE In Figure 11, "Application provisioning management" and "Application operation management" represent two activity areas, while the elements "Initiating", "Planning", "Executing", "Monitoring & controlling" and "Closing" represent sub-activity areas. The activities listed inside each sub-activity area are represented in Figure 10 by the element "Activity Label" and are listed in 6.2.1 to 6.5.6.

The Application management layer comprises processes from the governance knowledge domain carried out during the application provisioning and operation stages. Application provisioning management activities are carried out by project managers and organizational managers, during the provisioning stages of the application life cycle. Application operation management activities are related to the management and use of the application during the operation stages. As depicted in Figure 11 and in conformance with ISO/IEC 15288, the processes in both stages comprise project initiating, planning, executing, monitoring and controlling and closing.

6.2.2 Initiating

In accordance with ISO/IEC 15288, the objective of project initiating is to establish the requirements of the project to be undertaken. Once the project requirements are established the feasibility of the project is established by checking that the resources (personnel, materials, technology, and environment) required for executing and managing the project are available, adequate, and appropriate and that the time-scales to completion are achievable. As necessary, and by agreement of all parties concerned, the requirements of the project may be modified at this point to achieve the completion criteria.

Activity labels defined by the ASLCRM for this activity area include the following:

a) develop application project charter for its realization;

b) identify necessary skills;

c) identify stakeholders;

d) appoint application owner;

e) appoint application architect;

f) appoint application security architect;

g) manage knowledge;

h) develop, acquire or provide skills;

i) map application life cycles used in the organization to the reference model.

6.2.3 Planning

In accordance with ISO/IEC 15288, the objective of project planning is to prepare the plans for execution of the project. The plans associated with the execution of the project shall contain descriptions of the associated activities and tasks and identification of the software products that will be provided.

Activity labels defined by the ASLCRM for this activity area include the following:

a) develop project management plan;

b) collect requirements;

c) define scope;

d) plan the application security risk management;

e) plan project risk management;

f) create the work breakdown structure;

g) define activities;

h) sequences activities;

i) estimate activities resources;

j) estimate activities duration;

k) develop schedule;

l) estimate cost;

m) determine budget;

n) plan quality;

o) develop human resource plan;

p) plan communication;

q) plan procurements.

6.2.4 Executing

In accordance with ISO/IEC 15288, the objective of project execution is to carry out the project by executing the project plans established previously.

Activity labels defined by the ASLCRM for this activity area include the following:

a) direct and manage project execution;

b) perform assurance quality;

c) acquire project team;

d) develop project team;

e) manage project team;

f) distribute information;

g) manage stakeholder expectation;

h) conduct procurement.

6.2.5 Monitoring and controlling

In accordance with ISO/IEC 15288, the objective of project monitoring and controlling is to determine the status of the project and to ensure that the project performs according to plans and schedules, within projected budgets and it satisfies technical objectives.

Activity labels defined by the ASLCRM for this activity area include the following:

a) monitor and control project work;

b) perform integrated change control;

c) verify scope;

d) control scope;

e) control schedule;

f) control cost;

g) perform quality control;

h) report performance;

i) monitor and control risks;

j) administer procurements.

6.2.6 Closing

In accordance with ISO/IEC 15288, the objective of project closing is to complete and finalize the project activities.

Activity labels defined by the ASLCRM for this activity area include the following:

a) perform final review of unresolved issues;

b) perform a review of important problems solved and lessons learned;

c) submit this review back to relevant organization bodies for continuous improvement purposes;

d) close project of phase;

e) close procurement.

6.3 Application provisioning and operation layer

6.3.1 General

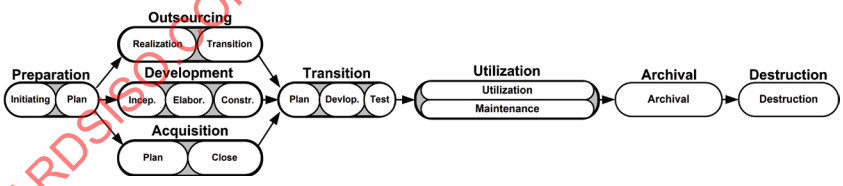

Figure 12 — Application Provisioning and Operation

The application provisioning and operation layer comprises activities from the software engineering domain related to the provisioning, maintenance, archival and destruction of the application. As recommended by standards such as ISO/IEC 12207, ISO/IEC 15288, ISO/IEC 37500, and ISO/IEC 15489 the relevant activity areas are preparation, outsourcing, development, acquisition, transition, utilization and maintenance, archival and destruction.

6.3.2 Preparation: Initiating

The objective of preparation: initiating is to carry out preliminary or preparation activities including the inception and planning of the development project. This includes deciding which parts of the implementation are realized through outsourcing, development and acquisition.

Activity labels defined by the ASLCRM for this activity area include the following:

a) Develop technical vision;

b) Validate the application scope contexts and specifications;

c) Identify and broadly categorize information which will be processed by the system;

d) Perform an initial high level application risk analysis;

e) Define security needs and the application targeted level of trust;

f) Select ASCs accordingly to this level;

g) Assess the costs and efforts related to security activities and to adding these concerns in regular project activities;

h) Define and acquire selected ASCs by the application targeted level of trust;

i) Define security and verification and measurement activities from the ASCs selected by the application targeted level of trust;

6.3.3 Preparation: Plan

The objective of preparation: plan is to plan activities realization including the inception and planning of the development project. This includes deciding which parts of the implementation are realized through outsourcing, development and acquisition.

Activity labels defined by the ASLCRM for this activity area include the following:

a) Define and plan the required stages and activities areas from the Application Security Life Cycle Reference Model;

b) Plan security and verification and measurement activities from the ASC selected by the application Targeted Level of Trust.

6.3.4 Outsourcing: Realization

In accordance with ISO/IEC 37500, the objective of outsourcing is to transfer part of or the entirety of application development to a third party. Outsourcing typically involves the following: identify outsourcing strategy and goals, validation of outsourcing strategy against business and project needs, specification of service requirements, and governance model and delivery.

Activity labels defined by the ASLCRM for this activity area include the following:

a) outsourcing preparation;

b) outsourcing advertisement;

c) supplier selection;

d) contract agreement;

e) agreement monitoring.

6.3.5 Outsourcing: Transition

Outsourcing typically involves a transition the following: identify outsourcing strategy and goals, validation of outsourcing strategy against business and project needs, specification of service requirements and governance model and delivery.

Activity labels defined by the ASLCRM for this activity area include the following:

a) acquirer acceptance; and

b) closure.

6.3.6 Development: Inception

In accordance with ISO/IEC 12207, the objective of development is to develop/construct part of or the entirety of the application. Inception typically involves the following: Initiate and validate the development project plan.

Activity labels defined by the ASLCRM for this activity area include the following:

a) initiate project;

b) plan and manage iteration;

c) identify and refine requirements;

d) agree on technical approach.

6.3.7 Development: Elaboration

In accordance with ISO/IEC 12207, the objective of elaboration is to develop/construct part of or the entirety of the application. Development typically involves the following: requirements analysis and definition, architectural design, detailed design, software construction, software integration, software qualification and testing.

Activity labels defined by the ASLCRM for this activity area include the following:

a) plan and manage iteration;

b) identify and refine requirements;

c) develop the architecture;

d) develop solution increment;

e) test solution;

f) ongoing tasks.

6.3.8 Development: Construction

In accordance with ISO/IEC 12207, the objective of construction is to develop/construct part of or the entirety of the application. Construction typically involves the following: requirements analysis and definition, architectural design, detailed design, software construction, software integration, software qualification and testing.

Activity labels defined by the ASLCRM for this activity area include the following:

a) plan and manage iteration;

b) identify and refine requirements;

c) develop solution increment;

d) test solution;

e) ongoing tasks.

6.3.9 Acquisition: Plan

In accordance to ISO/IEC 12207, the objective of planning an acquisition is to obtain the product and/or service that satisfy the need expressed by the acquirer. Acquisition begins with the identification of customer needs.

Activity labels defined by the ASLCRM for this activity area include the following:

a) acquisition preparation;

b) acquisition advertisement;

c) supplier selection;

d) contract agreement;

e) agreement monitoring.

6.3.10 Acquisition: Close

In accordance to ISO/IEC 12207, the objective of closing an acquisition is to close a acquisition once was validated the product and/or service that satisfy the need expressed by the acquirer. Acquisition ends with the acceptance of the product and/or service needed by the acquirer.

Activity labels defined by the ASLCRM for this activity area include the following:

a) acquirer acceptance;

b) closure;

6.3.11 Transition: Plan

In accordance to ISO/IEC 15288, the objective of transition is to establish a capability to provide services specified by stakeholder requirements in the operational environment. Transition activities install a verified application, together with relevant enabling systems, e.g. operating system, support system, operator training system, user training system, as defined in agreements. The objective of Transition: Plan is to establish a planning of the transition.

Activity labels defined by the ASLCRM for this activity area include the following:

a) plan iteration;

b) manage iteration;

c) assess results.

6.3.12 Transition: Development

In accordance to ISO/IEC 15288, the objective of transition is to establish a capability to provide services specified by stakeholder requirements in the operational environment. Transition activities install a verified application, together with relevant enabling systems, e.g. operating system, support system, operator training system, user training system, as defined in agreements. The objective of Transition: Development is to implement the transition.

Activity labels defined by the ASLCRM for this activity area include the following:

a) design the solution;

b) implement developer tests;

c) implement solution;

d) run developer tests;

e) integrate and create build.

6.3.13 Transition: Test

In accordance to ISO/IEC 15288, the objective of transition is to establish a capability to provide services specified by stakeholder requirements in the operational environment. Transition activities install a verified application, together with relevant enabling systems, e.g. operating system, support system, operator training system, user training system, as defined in agreements. The objective of Transition: Test is to verify the success of the transition.

Activity labels defined by the ASLCRM for this activity area include the following:

a) implement tests;

b) run tests.

6.3.14 Utilization: Utilization

In accordance to ISO/IEC 15288, the objective of utilization is to use the application in order to deliver its services. Utilization activities assign personnel to operate the application, and monitor the services and operator-application performance. In order to sustain services they identify and analyse operational problems in relation to agreements, stakeholder requirements and organizational constraints.

Activity labels defined by the ASLCRM for this activity area include the following:

a) identify organization processes impacted by the application;

b) adapt relevant organization processes to the application;

c) define roles;

d) identify information groups (records);

e) access application risk analysis;

f) assign roles, responsibilities, qualifications and permissions;

g) approve and manage access requests;

h) provide training to users;

i) execute application's processes and services;

j) fulfill requests;

k) manage incidents;

l) manage problems;

m) manage access;

n) manage events;

o) manage changes request;

p) perform responsive and operational validation;

q) monitor and control application's activities;

r) monitor and control application's ressources utilization.

6.3.15 Utilization: Maintenance

In accordance to ISO/IEC 15288, the purpose of maintenance is to sustain the capability of the application to provide a service. Maintenance activities monitor the application's capability to deliver services, record problems for analysis, take corrective, adaptive, perfective and preventive actions and confirm restored capability.

Activity labels defined by the ASLCRM for this activity area include the following:

a) maintenance responsibility and communications;

b) maintenance information gathering findings;

c) maintenance action plan;

d) maintenance process and service definition;

e) maintenance training;

f) maintenance process performance;

g) maintenance innovation and deployment;

h) event and request management;

i) maintenance planning;

j) requests and events monitoring and control;

k) SLA and supplier agreements management;

l) predelivery and transition services;

m) operational support services;

n) software evolution and correction services;

o) verification and validation;

p) configuration and version management;

q) process, service and software (product) quality assurance;

r) maintenance measurement and analysis;

s) causal analysis and problem resolution;

t) software rejuvenation, migration and retirement.

6.3.16 Archival: Archival

In accordance with ISO/IEC 15489, the objective of archival is the recordkeeping of all relevant paper and electronic records. This includes assuring that records are properly maintained, easily accessible and correctly documented from their creation right through to ultimate disposal.

Activity labels defined by the ASLCRM for this activity area include the following:

a) define and review organization acquisitions policy;

b) define data retention policies;

c) record access;

d) preserve records;

e) control archival use;

f) promote archives;

g) manage archiving administrative service;

h) manage archiving educational and research service;

i) manage archiving publicity and public programs.

6.3.17 Destruction: Destruction

In accordance with ISO/IEC 15288, the objective of disposal is to end the existence of an application. Disposal activities deactivate, disassemble and remove the system and any waste products, consigning them to a final condition and returning the environment to its original or an acceptable condition.

Activity labels defined by the ASLCRM for this activity area include the following:

a) define general disposal schedules;

b) define records classification and retention schedules;

c) define operational records disposal schedules;

d) define transfer of ownership and custody schedules;

e) define normal administrative practice;

f) define recordkeeping practices;

g) define a disposal action practice;

h) manage machinery of organization changes;

i) determine the disposal action;

j) authorize records destruction;

k) manage recordkeeping practices;

l) prepare records for destruction approval;

m) select the records removal process;

n) perform the records removal process;

o) perform the records removal verification process;

p) monitor and review records management performance;

q) report key performance information to management;

r) implement a regular reporting regime to enable the monitoring and reviewing of records management performance;

s) perform a records management assessment survey.

6.4 Infrastructure management

6.4.1 General

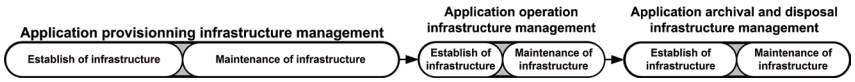

Figure 13 — Infrastructure management

This layer comprises activity areas relating to the organization's IT service management infrastructure supporting the application. Such activities are usually recommended by standards such as ISO/IEC 20000. The purpose of Infrastructure Management is to provide the enabling infrastructure and services to projects to support organization and application's project objectives throughout the life cycle. It typically consists of three activity area: Application provisioning infrastructure management, Application operation infrastructure management, and Application archival and disposal infrastructure management, each one containing two distinct activity sub areas: establishment of infrastructure and maintenance of infrastructure.

6.4.2 Establishment of the infrastructure

In accordance with ISO/IEC 15288, the objective of establishing the infrastructure is to define the project infrastructure requirements and business constraints that influence and control provision of infrastructure resources and services for the project. It includes identifying, obtaining and providing infrastructure resources and services that are needed to implement and support the application provisioning and operation.

Activity labels defined by the ASLCRM for this activity area include the following:

a) adjust, prepare and setup the development, tests, operational and archival environments;

b) draw up and update configuration documents;

c) validate and update the continuity plan and contingency plans;

d) draw up user handbook;

e) draw up administrator handbook;

f) adjust corporate procedures and policies impacted by the on lining of the system and inform actors and stakeholders affected by these changes;

g) proceed with acceptance tests for the main global functionalities.

6.4.3 Maintenance of the infrastructure

In accordance with ISO/IEC 15288, the objective of maintaining the infrastructure is to continuously or routinely communicate with projects to determine the degree to which delivered infrastructure resources satisfy their needs. It involves identify and providing the improvements or changes to the infrastructure resources as the project requirements change. This is typically carried iteratively using plan-do-check-act process cycles.

Activity labels defined by the ASLCRM for this activity area include the following:

a) maintain the system at the expected degree of trust;

b) apply best practices in identity and configuration management;

c) perform periodically audits and internal security tests;

d) perform changes control;