ISO/IEC JTC 1/SC 22 N 4309

2008-01-31

Replaces

ISO/IEC JTC 1/SC 22
Programming Languages

Document Type:	**Working Draft**
Document Title:	**Text for ISO/IEC WD 27034 – Information technology – Security techniques – Application security – Part 1: Guidelines to application security**
Document Source:	**SC 27 Secretary**
Project Number:	
Document Status:	**This document is circulated for review and comment. The SC 27 Secretary has requested that SC 22 members review this text, and if provide comments, if there are any. Please submit your comments to the SC 22 Secretary (sseitz@ansi.org) by the due date indicated, and they will be forwarded to SC 27.**
Action ID:	**COM**
Due Date:	**2008-03-31**
No. of Pages:	**45**

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC 1/SC 27 **N6274**

ISO/IEC JTC 1/SC 27/WG 4 **N46274**

REPLACES: N5737

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: text for Working Draft

TITLE: **Text for ISO/IEC Working Draft 27034 -- Information technology -- Security techniques -- Application security -- Part 1: Guidelines to application security**

SOURCE: Project Co-editors (Luc Poulin & Bruno Guay)

DATE : 2008-01-30

PROJECT: 27034-1

STATUS: In accordance with resolution 3 (see SC 27 N6017) of the 3rd SC 27/WG 4 meeting held in Lucerne (Switzerland), 1st - 5th October 2007, this document is being circulated for **STUDY AND COMMENT**.

The national bodies and liaison organizations of SC 27 are requested to send their comments/contributions on this Working Draft directly to the SC 27 Secretariat by **2008-04-01.**

PLEASE NOTE: For comments please use **THE SC27 TEMPLATE** separately attached to this document.

ACTION: **COM**

DUE DATE: **2008-04-01**

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-chair
E. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 43

Secretariat ISO/IEC JTC 1/SC 27 -
DIN Deutsches Institut für Normung e.V., Burggrafenstrasse 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de
HTTP://www.jtc1sc27.din.de/en

ISO/JTC 1/SC 27 N6276

2008-01-02

ISO/IEC WD 27034-1

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

Draft, Information technology — Security techniques —Application security — Part 1: Guidelines to application security

Technologie de l'information — Techniques de sécurité — Partie 1: Directives dans la sécurité des applications

Document type: International standard
Document subtype:
Document stage: (40) Enquiry
Document language: E

D:\Mes documents\CRIM-ISIQ\Comités\JTC1-SC27 ISO\WG4 - Security Controls and Services\ISO 27034 - Application Security\3_Working Draft\1st_WD - Japan\SC27N6276_Working_Draft_27034_Part1_Feb2008-01-29e.doc
ISO Basic template Version 3.0 1997-02-03

Contents

Figures

Note:

⇒ *Paragraphs in italic-blue preceded by an arrow are comments and notes from editors. These will hopefully be progressively replaced by actual content in further revisions.*

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27034-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

ISO/IEC 27034 consists of the following parts, under the general title *Information technology — Security techniques — Application security*:

Part 1: Guidelines to application security

0.1 Introduction

Today's organisations know they must protect their information, applications and IT infrastructure in order to stay in business. They are increasingly protecting themselves by operating formalized information security management systems. At the technical level they protect themselves with firewalls, antivirus and intrusion detection systems. Their recovery and incident response plans ensure business continuity, while periodic audits and penetration tests verify overall security. In addition user staff performs checks on the results of processing to determine the correctness of the data and the information produced by the systems.

However, perimeter and IT infrastructure protection is generally insufficient. For instance, a firewall may not provide adequate protection against vulnerabilities resulting from faulty software. This kind of security fault can only be fixed by a software patch from the development team. The fact is, all security problems that can be solved with a software patch are application security problems.

Furthermore, a once secure application may become unsecured if new functionalities are added or programming errors, are corrected during its production phase. Mismanagement of the application can have the same impact.

A systematic approach to application security is necessary to guarantee to an organization adequate protection of the information used by its applications, and as a requirement to support an effective information security management system (ISMS) as described in ISO/IEC 27001.

A secure application is an application that properly covers security needs from the management, IT, development and audit points of vew, according to a target level of trust, taking into account the security requirements coming from the type of data, the target execution context (legal, business and technological), the actors and the application characteristics.

It must be possible to obtain evidence that the target level of trust was attained and maintained.

If the development team, including the evolution team who develops new functionalities on an existing application, can integrate security requirements and best practices within the application life cycle, the cost on the security integration can be minimized and the risk of security breaches can be reduced from the beginning of the application design and development. At a minimum, common security vulnerabilities resulting from insecure coding and development practices can be eliminated to provide a more secure and resilient code base.

0.2 Objectives

The objective of this standard is to provide guidance and promote best practices about emerging and existing security issues concerning the software application life cycle, including software development.

The standard is targeted for use by software application developers and understandable by managers and auditors.

The standard will provide an organisation with methods for establishing security requirements, assessing security risks, identifying a desired level of trust, selecting security measures and controls, and developing their own guidelines.

0.3 Targeted Audiences, Values & Benefits

This standard will be useful for organisations of all sizes. The following actors will find values and benefits:

0.3.1 Line management

Information security managers, project managers, administrators, application holders, user managers, etc. who need to:

- manage the cost of implementing and maintaining application security in relation to the risks and value of an application for the organisation;
- prove that the application has attained and maintained a targeted level of trust;
- implement a secure application;
- identify the adequate level of trust according to the context;
- discover what security measures and control points should be implemented and tested;

0.3.2 Developers

Architects, analysts, programmers, testers, etc. who need to:

- know what Application Security Measures should be applied at each phase of the application life cycle and why they should be;
- identify control points and safety functions to be implemented;
- minimize the impact of introducing security in their development, test and documentation processes;
- get access to tools and best practices to speedup development;
- facilitate peer review.

0.3.3 Auditors

Auditors who need to:

- know the scope and process of verification;
- make audit results repeatable;
- get a list of controls needed to prove the application has reached the required level of trust;
- standardize the application security certification;
- minimize the certification cost.

0.3.4 End-users

Employees and any end users who need:

- assurance that it is deemed secure to use the application;
- assurance that the application will produce reliable results consistently and in a timely manner;
- assurance that the security measures and controls and in place and function correctly as expected.

0.4 Principles

0.4.1 Adequate application security cost

The cost of application security should be appropriate to the targeted level of trust approved by the organisation.

0.4.2 Application security is context dependent

⇒ *Application security is an affirmation that depends on the context of an organisation. An organisation can claim an application is secure, but this affirmation is only valid for this organisation.*

0.4.3 Application security must be demonstrated

⇒ *An application is considered secure at a specific time, when it passes all security controls as expected.*

⇒ *An application cannot be declared secure if the organization cannot obtain the required evidence that the implemented security controls adequately address the security requirements.*

⇒ *The term "security control" refers to the specific measurement activity that is an integral part of any application security measure.*

0.4.4 Application security scope

⇒ *To be able to have a good understanding of the implications of the Application Security, we must well define the application security Scope.*

⇒ *Application security is to protect the data computed, used, stored and transferred by an application as requested by the organisation. This protection may ensure not only the availability, integrity and confidentiality of the data, but also the authentication and the non-repudiation of the users who will access it.*

⇒ *To ensure application security, it must guaranteed that the data computed and stored by this application is correctly protected by the application in its execution contexts.*

⇒ *To do that, application security may also require some physical, hardware or product security controls.*

Application Security — Part 1: Guidelines to Application Security

1 Scope

This standard provides a life cycle for the business manager to securely define, develop if necessary, implement, manage, and retire an application.

From the business manager point of view, an application can be an internal, outsourcing or product application.

More precisely, this standard:

- provides guidelines to assist organisations in identifying security activities and controls in all phases of a software application lifecycle;
- is intended to be helpful to any organisation wishing to obtain assurance that a software application has reached and maintains a targeted level of trust;
- applies to the application software itself and to surrounding factors that have an impact on the security of the application, such as data, technology, processes and actors;
- provides guidelines to establishes reference technical criteria for organisations sub-contracting to third parties the development of secure applications.

This standard does not:

- provide guidelines for physical and network security;
- provide secure coding specifications in any programming language.

This standard is not:

- a new software application development standard;
- a new application project management standard.

2 Normative references

- ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security management
- ISO/IEC 12207:2006 Draft, Information technology – Software life cycle process
- ISO/IEC 15288:2007, Information technology – System Life Cycle Processes
- ISO/IEC 21827:2007 "Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM®)" JTC1/SC27
- ISO 27033, ISO/IEC PDTR 24748, ISO/IEC TR 19760, ISO/IEC TR 15271, ISO/IEC 27000.

3 Terms and definitions

For the purposes of this standard, the following terms and definitions apply:

3.1
Actor

Someone or something initiating interaction with any process in the application security lifecycle or any process in the business application.

3.2
Application

Software designed to help users perform particular tasks or handle particular types of problems, as distinct from software that controls the computer itself.

See : Terms and definitions 2.6 - ISO/IEC 18019 - Software and system engineering – Guidelines for the design and preparation of user documentation for application software

Application software is a subclass of computer software that employs the capabilities of a computer directly to a task that the user wishes to perform. This should be contrasted with system software which is involved in integrating a computer's various capabilities, but typically does not directly apply them in the performance of tasks that benefit the user. In this context the term application refers to both the application software and its implementation.

We consider the DBMS and any other involved product to be part of the application.

Synonym: application software

3.3 Business application

A business application is an application that helps an organisation to automate a business process or function. Business processes include people and technologies.

3.4
Life cycle

The evolution of a system, product, service, project or other human-made entity from conception through retirement. [See ISO/IEC 12207:2006 Draft]

3.5
Life cycle model

A framework of processes and activities concerned with the life cycle, which also acts as a common reference for communication and understanding. [See ISO/IEC 12207:2006 Draft]

3.6
Secure Application

A secure application is an application that properly covers security needs from the management, IT, development and audit points of view, according to the level of trust desired, taking into account the type of data and the target execution context. It must be possible to show supporting evidence to demonstrate that the target level of trust was reached.

3.7
User

An actor or group that interacts with an application during its lifecycle.

NOTE: For the purposes of application security, a user may be an end-user, a system administrator, a DBA, etc. We will not differentiate between these user types because the access of all these users must be controlled.

3.8
Verification

Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled.

NOTE

1. Verification in a life cycle context is a set of activities that compares a product of the life cycle against the required characteristics for that product. This may include, but is not limited to, specified requirements, design description and the system itself.

[See ISO/IEC 12207:2006 Draft]

4 Structure of this standard

PART 1 – Guidelines to Application Security: Overview, Concepts, and Principles

This document presents an overview of application security. It introduces definitions, concepts, principles and the overall application security process.

PART 2 – Application Security Lifecycle

This document presents… (to be completed…)

2.1 – Organisational Normative Framework

This document presents the Organisational Normative Framework (ONF), its contents and the processes for creating, maintaining and adapting it to the organisation's needs and contexts.

2.2 – Application Risk Management

This document presents an application risk analysis process that will examine an application's characteristics in order to identify the targeted application level of trust required by the organisation according to its specific business, legal and technological contexts.

⇒ *Investigate link with content of, and possible change request to ISO 27005. – To be discussed in Kyoto.*

2.3 – Application Normative Framework

This document presents the Application Normative Framework (ANF) and the process for creating it from the ONF for a specific application project, according to the application's contexts, characteristics and the targeted level of trust obtained from the risk analysis.

2.4 – Application Security Lifecycle

This document presents the application security lifecycle processes and how to associate them to the software and system processes involved in an application project. It also identifies actors involved in these processes by identifying their roles, responsibilities and qualifications.

PART 3 – Architecture, Design, and Development

PART 4 – Protocols and Data Structure

This document will present the XML Schema for the Application Security Measure (ASM). It will be used to validate the XML data structure of ASMs and other components of the standard, and to help automate distribution, update and use of ASMs.

PART 5 – Application Security Assurance

This document presents the application security assurance and certification process that will measure the actual application level of trust and compare it with the targeted application level of trust previously identified by the organisation.

⇒ *Investigate link with content of, and possible change request to ISO 270xx. – To be discussed in Kyoto.*

Part 6 – Security guidance for specific application

6.1 – N-Tier and Web Applications Security

This document will present, on a practical approach, the:

N-Tier-and-Web-Specific Risks

N-Tier-and-Web-Specific ASMs

N-Tier-and-Web-Specific Standards

6.2 – Client/Server Applications Security

This document will present, on a practical approach, the:

Client/Server-Specific Risks

Client/Server-Specific ASMs

Client/Server-Specific Standards

5 Standard Overview

This standard presents the required components, processes and frameworks that will help an organisation acquire, implement and use applications it can trust, at an acceptable security cost. More specifically, these will provide measurable evidence that applications reach and maintain a target level of trust.

All these components, processes and frameworks are part of an overall process called the Application Security Management Process.

5.1 Application Security Management Process

To implement an Application Security Management Process (ASMP) the organisation will have to create a committee who will manage this overall application security process. This ASMP committee will ensure the process is the answer to the organisation's application security concerns and that it is applied to all application projects in the organisation.

The Application Security Management Process is performed in five steps.

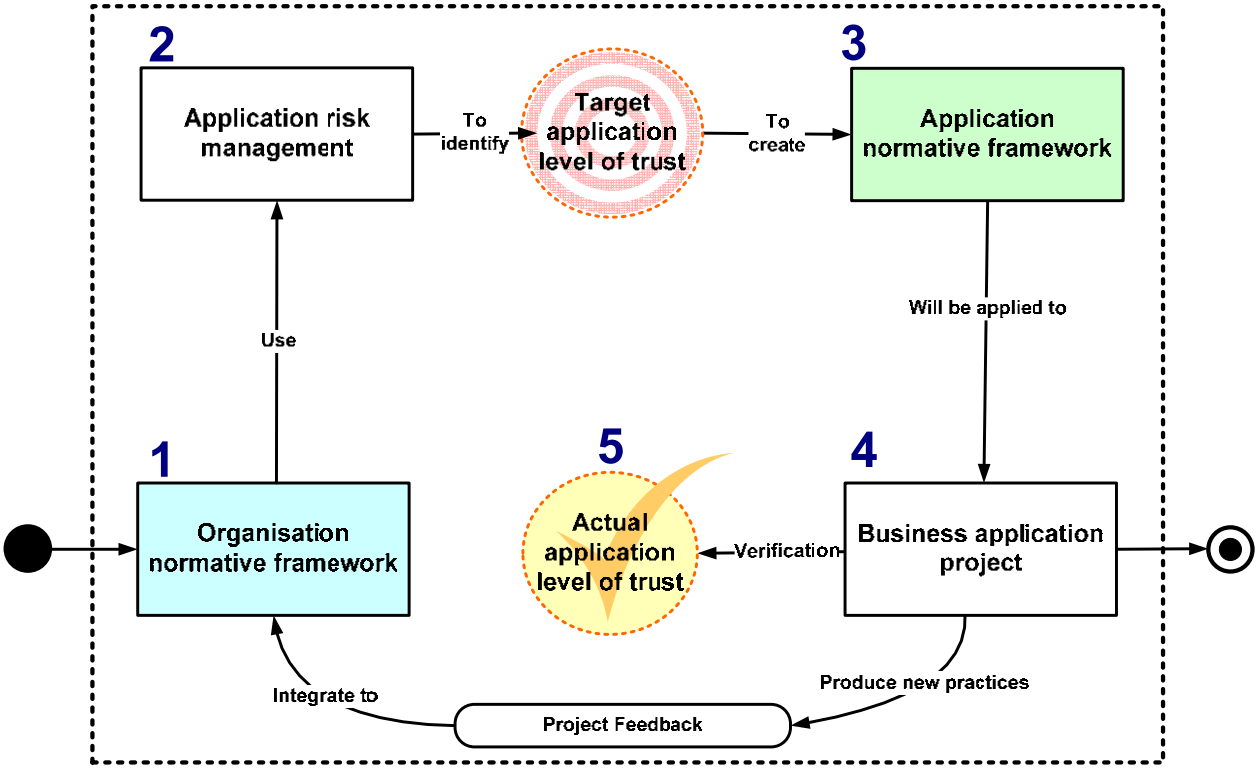

Figure 1 – Application Security Management Process

5.1.1 Organisation Normative Framework

The first step of the ASMP involves the Organisation Normative Framework (ONF). This framework contains all the regulations, laws, best practices, roles and responsibilities accepted by the organisation. It defines all organisation contexts and becomes the unique organisation referential for application security.

Prior to its first use, the ONF will be created by an ONF committee which will also be responsible for maintenance of the ONF.

This step of the ASMP and its associated components and processes will be presented in subclause 6.1

5.1.2 Application Security Risk Management

The second step of the ASMP involves the Application Security Risk Management (ASRM).

The purpose of this step is to receive the organisation's approval on a targeted level of trust for the business application, and periodically revise this target in the course of the project.

The organisation may already have implemented an enterprise-level risk analysis process, but a specific application-oriented risk analysis must be performed for each business application project.

As part of the creation of the Organisation Normative Framework, the organisation must have selected an adequate ASRM process for the organisation's business application projects. A verification team will verify that this process is used correctly.

This step of the ASMP and its associated components and processes will be presented in subclause 6.2

5.1.3 Application Normative Framework

The third step is to identify all the relevant elements from the Organisation Normative Framework that will apply to a specific business application project. This results in the Application Normative Framework (ANF). The targeted application level or trust, the application contexts (legal, business and technological), the actors and the application characteristics will determine the exact contents of the ANF.

This step will also define the Application Security Lifecycle (ASL) for the business application project. The ASL will be a subset of a Generic Application Security Lifecycle (GASL) contained in the ONF. For a specific application project, the ASL will contain only the processes and security measures from the GASL that were selected according to the targeted level of trust, the organisation's needs, the application contexts and characteristics. The ASL is a component of the ANF.

This step of the ASMP and its associated components and processes will be presented in subclause 6.2.5.2

5.1.4 Business Application Project

The fourth step is the actual use of the Application Normative Framework in the business application project. The execution team will implement the security activities contained in the ANF.

This step of the ASMP and its associated components and processes will be presented in subclause 6.4

5.1.5 Application Security Verification

The last step is the Application Security Verification process. This process may be performed by an internal or an external verification team, using the controls provided by the Application Normative Framework.

The purpose of this step is to verify and provide evidence that an application has reached and maintained the targeted level of trust. It will measure the actual application level of trust at a specific time. Depending of the level of trust needed for the particular application project, this process may be unique, periodic, or event-driven.

This step of the ASMP and its associated components and processes will be presented in subclause 6.5

5.2 Impact of this standard on a business application project

Figure 2 shows an overview of roles and responsibilities in a typical application project.

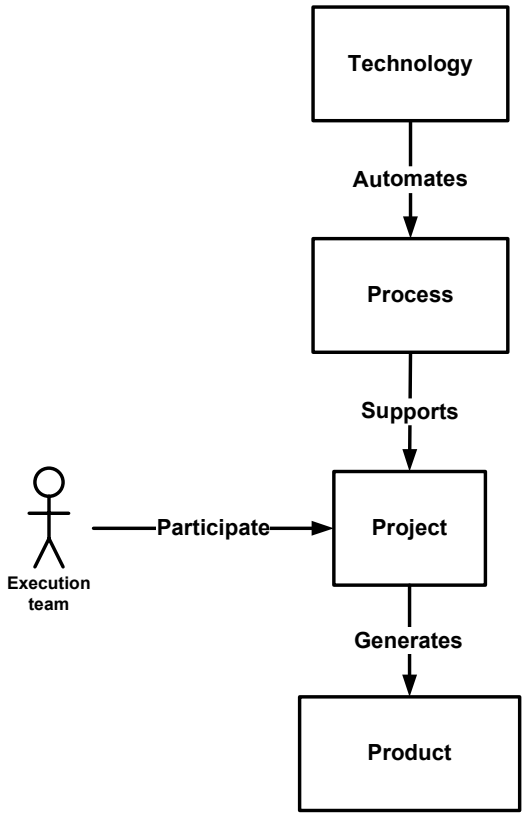

Figure 2 – Roles and responsibilities in a typical application project

Figure 3 shows how this standard adds new roles and responsibilities, along with key components of the standard: the ONF and the ANF.

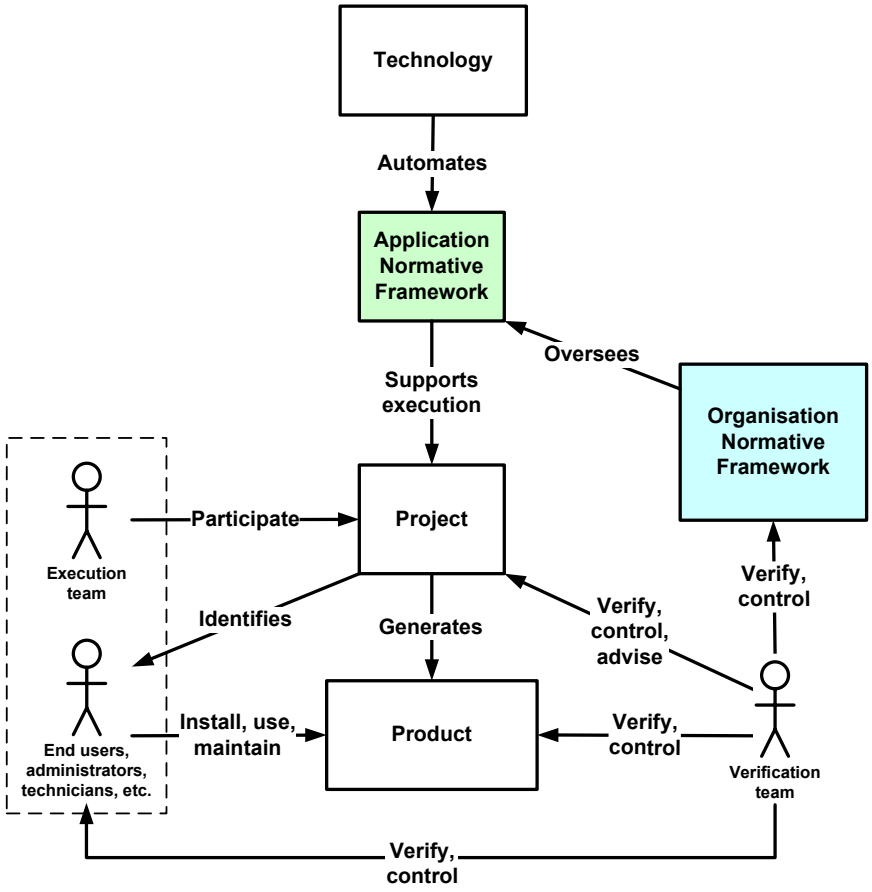

Figure 3 – Impact of this standard on roles and responsibilities in a typical application project

Figure 3 shows clearly that the ONF, an organisation-level component, is not acting directly on the business application project. The execution team, the verification team and the users will only be impacted by the ANF, a project-level component that contains precise and detailed security measures and controls.

Although the verification team has the responsibility to verify the ONF, this is not done as a part of the business application project.

6 Concepts

Clause 6 further develops the concepts of the ISO 27034 standard presented in the overview.

6.1 Organisation Normative Framework

6.1.1 Presentation

The Organisation Normative Framework (ONF) is an organisation-level framework where all application security best practices recognized by the organisation will be stored and referred from. It comprises essential components, processes that utilize those components, and processes for managing the ONF itself.

The ONF is the foundation of application security in the organisation and all future application security decisions will be made by referring to this framework. For example, code reviews can only be performed in a project if coding guidelines can be found in the ONF.

Figure 4 shows a high-level view of the ONF contents.

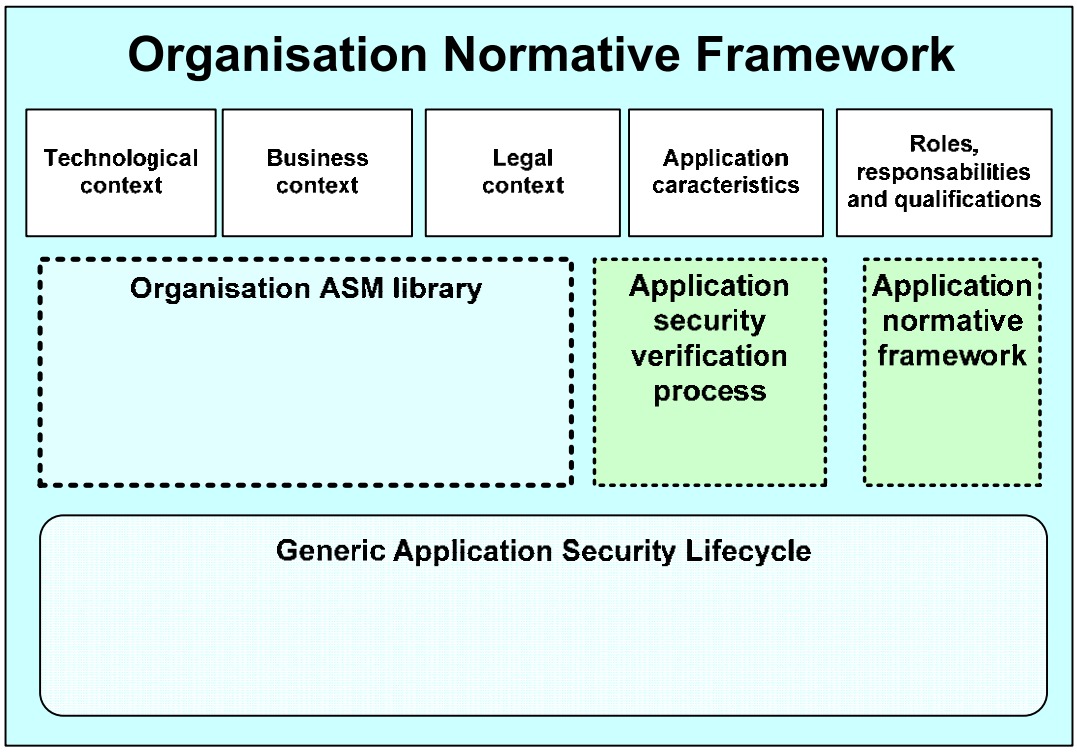

Figure 4 – Organisation Normative Framework (simplified)

An organisation must have a formal ONF, which must contain the following components.

6.1.2 Components

6.1.2.1 Technological context

The technological context is an inventory of all products and technologies available for application projects in the organisation.

The technological context includes computers, tools, products, communication infrastructure and other technical devices. Examples of technological contexts that may have an impact on application security: client-server infrastructure, web infrastructure, network infrastructure, development environment and tools, etc.

The technological context also determines the available technological security measures. For example, if the infrastructure that the business application will be run in can not support bi-directional TLS 1.0 authentication then it is not possible to implement that measure for the application. The organisation will have to select another measure for bi-directional authentication, if that functionality is needed at the target level of trust.

The technological context should include:

- **Technologies used by the organisation**

  This inventory will be continuously maintained by feedback from projects

- **Technologies needed by an application**

  This comes from new functional requirements identified in the course of a business application project. This need should be added to the ONF and an organisational process should ensure that approved technologies are found to fulfil the new requirements.

- **Technologies available**

  This comes from research, trend analysis, technological watch.

6.1.2.2 Business context

The business context is a list and documentation of all standards and best practices adopted by the organisation that may have an impact on business application projects.

The business context includes:

- people involved in the development, maintenance and usage of the application;
- processes such as project management process, development process, risk analysis process, operational processes, verification and control processes;
- the normative framework for the business domain;
- the development methodology used in the organisation;
- the best practices for all programming languages used in the organisation;
- the organisation formal project management process.

6.1.2.3 Legal context

The legal context is a list and documentation of all laws and regulations that may have an impact on business application projects, in any of the organisation's business locations. The legal context includes laws, rules and regulations of the countries where the application is developed and/or is used.

An organisation using the same application in two different countries may have to meet different security requirements.

6.1.2.4 Application characteristics

Application characteristics are a list and documentation of the organisation's usual functional requirements and corresponding pre-approved secure solutions. Application characteristics should include:

- the information computed, stored and transferred by the application;
- the application functionalities, services and requirements;
- the roles of all users, including the end-users and users such as administrators, technical support, DBAs, etc.
- the source code, the binary code, and products used by the application;
- risks for the organisation to use this application;

- target level of trust needed by the organisation for this application instance.

Additional characteristics may include how the application interacts with:

- other systems;
- the runtime infrastructure upon which it depends;
- the number of controls of the environment upon which the application will run.

6.1.2.5 Roles, responsibilities and qualifications

This is a list and documentation of all roles, responsibilities and required qualifications for actors involved in the organisation's security application lifecycle. This is an organisational-level policy that will help ensure that critical roles for all processes are filled, that responsibilities are defined, that conflicts of interest are avoided, and that people filling the roles have sufficient qualifications.

6.1.3 Organisation ASM Library

A list and documentation of all Application Security Measures (ASMs, defined in subclause 6.1.5) used by the organisation, attached to the standards, best practices, actors, users, contexts and application characteristics that they evolved from, in relation to the organisation's defined levels of trust;

From this library will be selected the ASMs needed for any specific business application project.

Figure 5 shows a simple example of an Organisation ASM Library.

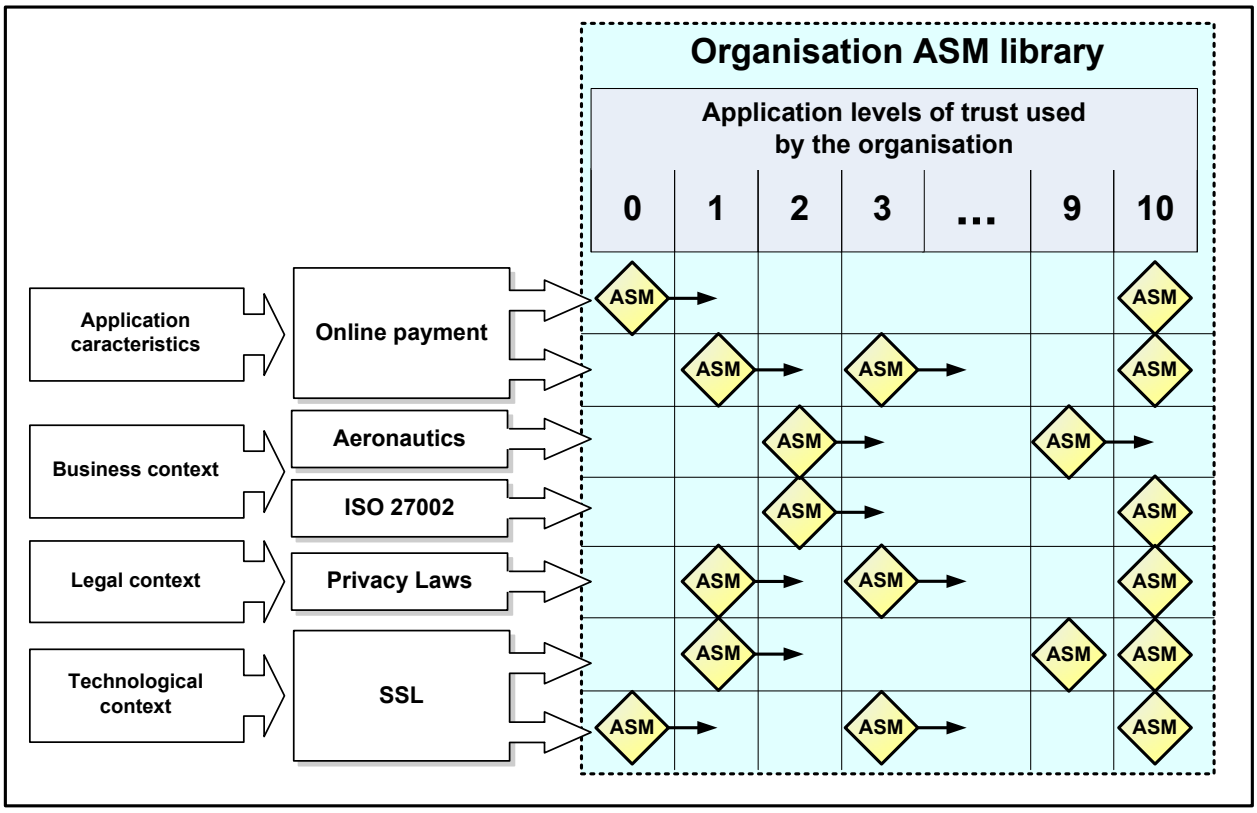

Figure 5 – Example of an Organisation ASM Library (part of ONF)

The example shows how the organisation's usual application characteristics and contexts have determined the ASMs used on the different levels of trust. In this example, the organisation uses 10 levels of trust.

6.1.4 Application level of trust

The organisation must define its own range, or scale, of levels of trust that can be selected as a target for business applications.

Example: An organisation might use, as in the example in Figure 5, numeric levels from 0 to 10. Another organisation might use a domain of defined values such as [low, medium high], [green, yellow, red] or [public, proprietary, sensitive, restricted, secret, top secret].

The organisation must define a minimum acceptable level of trust for any of its business applications, for which this standard will use the name “level of trust zero”. The organisation may use any name for this level of trust.

No application project in the organisation shall be allowed to reach a level of trust lower than level of trust zero.

In the example in Figure 5, the ONF committee has defined an ASM at level zero for any business applications using online payment. Even if the risk analysis for this application resulted in a target level of trust zero, this ASM shall still be performed.

6.1.5 Application Security Measure

The Application Security Measure (ASM) is a central concept in this standard. It is the tool used to actually implement application security and verify the result.

The ASM provides both a security activity (what has to be done for reducing a specific security risk) for the execution team and a control (what has to be done for making sure the activity has been successfully performed) for the verification team.

Figure 6 shows the ASM used as a control in a business application project by the verification team.

An ASM is a complex data structure which will be explained below and further detailed in the document “PART 4 – Protocols and Data Structure”

⇒ *Present the principle that all security activities must be controlled in order to obtain evidence that the measure worked as expected.*

⇒ *Present the concept of ASMs linked together in a graph, so that performing the activity in an ASM must be followed by the activity of children ASMs. This ensures that the organisation can prevent the execution team from bypassing critical security activities.*

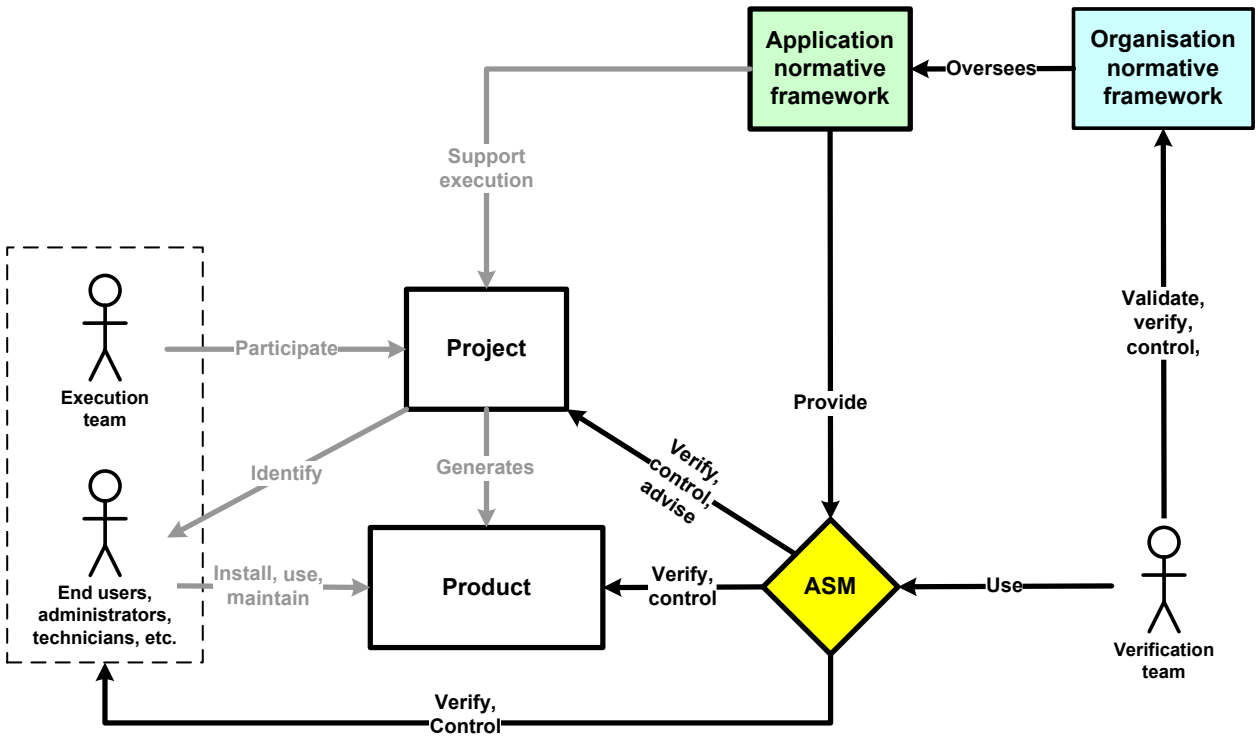

Figure 6 – ASM used as a control

⇒ *Explain how an ASM will help to verity and control, the processes of the project, the actors and the product itself. For example:*

An ASM

- May cover all elements inside the application security scope
- May address the application product (components), including software, data, COTS and infrastructure verification
- May address all processes in the application security lifecycle
- May address all actors and roles, responsibilities and qualifications

6.1.5.1 ASM Structure

The application Security Measure (ASM) contains four parts: Identification, Objective, Activity and Control.

6.1.5.1.1 ASM Identification

The ASM identification section will contain information such as :

- ASM information: ASM name, ID, Author, date, description, etc.
- Pointers to parent and children ASMs (the ASM is a graph structure; these details will be further explained in the document “PART 4 – Protocols and Data Structure”).
- Pointers to the relevant contexts and application characteristics that provided the requirements for this ASM (see Figure 5**).**
- Version of ASM XML Schema: Version number (a XML schema will be made available for a formal description of the ASM structure; these details will be further explained in the document “PART 4 – Protocols and Data Structure”)

6.1.5.1.2 ASM Objective

The ASM objective specifies why this ASM exists. It identifies the needs for the manager, the team leader, the development team, the auditor, etc.

The objective also details what will be evaluated, and on which level of trust, application characteristics or requirements this ASM is active.

An ASM may be associated to many levels of trust. In the example in Figure 5**,** an ASM has been defined at level zero for any business applications using online payment. This ASM is mandatory for all projects when the target level of trust is 0 to 9. If the target level of trust is 10, a different ASM is used.

The objective provides links to standards to which this ASM is associated (for example: ITIL, Cobit, ISO 27002, RUP, design pattern name, etc.) including the phase name of each standard.

6.1.5.1.3 ASM Activity

This part describes the processes or procedures needed to implement the measure.

The question of “when” the activity will occur is addressed by providing a pointer to a phase of the Generic Application Security Lifecycle (defined in subclause 6.1.7).

Other information contained in this part:

- Complete description of the security activity.
- The activity complexity level and the required qualifications for actors.
- Artefact produced by this activity.
- Expected results (situation, status or precise artefact value description).
- The cost to perform this activity.

6.1.5.1.4 ASM Control

This part presents the control that will be performed for verification of the related ASM activity.

The question of "when" the control will occur is addressed by providing a pointer to a phase of the Generic Application Security Lifecycle (defined in subclause 6.1.7).

- Complete description of the control
- The complexity level of the control and the qualifications required for actors who will perform the control.
- The cost to perform the control. May specify that a periodic control will be required.

6.1.5.1.5 Pointers to other components in the ONF

As described in preceding paragraphs, the ASM will include pointers to other components in the ONF. These pointers allow the author to provide such information as "why this ASM exists", "when does the activity occur", "when is the control performed".

Figure 7 shows a graphical representation of these pointers.

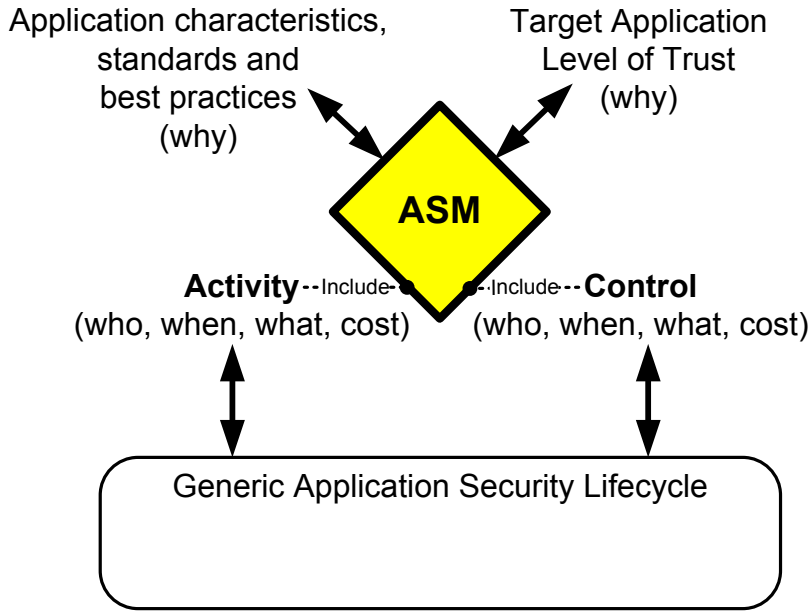

Figure 7 – The four pointers in an ASM

6.1.6 Application Normative Framework

The Application Normative Framework (ANF) contained in the ONF is a template used as a basis for all application projects. It contains all the ASMs included in level of trust zero, which is defined as the minimum acceptable level of trust the organisation will accept. The ASMs included at level zero can not be removed during an application project.

For each application project, this template will be copied from the ONF, and completed with the relevant contexts, application characteristics and ASMs needed for the project.

The result will be a project-specific, customized ANF which will be used by the project execution team and verification team. This is further discussed in subclause 6.2.5.2.

6.1.7 Generic Application Security Lifecycle

An organisation whose business involves business applications (either developing, outsourcing or acquiring applications) habitually uses a collection of processes (development process/methodology,

acquisition process, transition process, etc). For the purposes of this standard, this collection of processes will be named “Application Security Lifecycle (ASL)”. It presents a process-oriented view of application security activities and controls.

The Application Security Lifecycle (ASL) is usually unique and customized for a particular organisation. It has often been in use for quite some time and has been refined over the years. It is NOT a new concept brought by this standard.

This standard does not impose or even recommend a change in the organisation’s ASL. This standard instead adds components called “Application Security Measures” (ASMs) to the organisation’s ASL.

As previously discussed in subclause 6.1.5.1.5, ASMs include pointers to processes in the lifecycle, thus specifying when security activities and controls must be performed.

There are so many possible ASLs already in use in the industry that it is neither possible nor desirable for this standard to refer to all of them. It is thus impossible to have an ASM in the standard point directly to a process in an ASL. This would make the ASM non-portable, useful for a single organisation only.

The solution to this problem is to define a Generic Application Security Lifecycle (GASL) as a standardized way of representing the ASL for all organisations. **Fehler! Verweisquelle konnte nicht gefunden werden.** Figure 8 shows the GASL proposed by this standard.

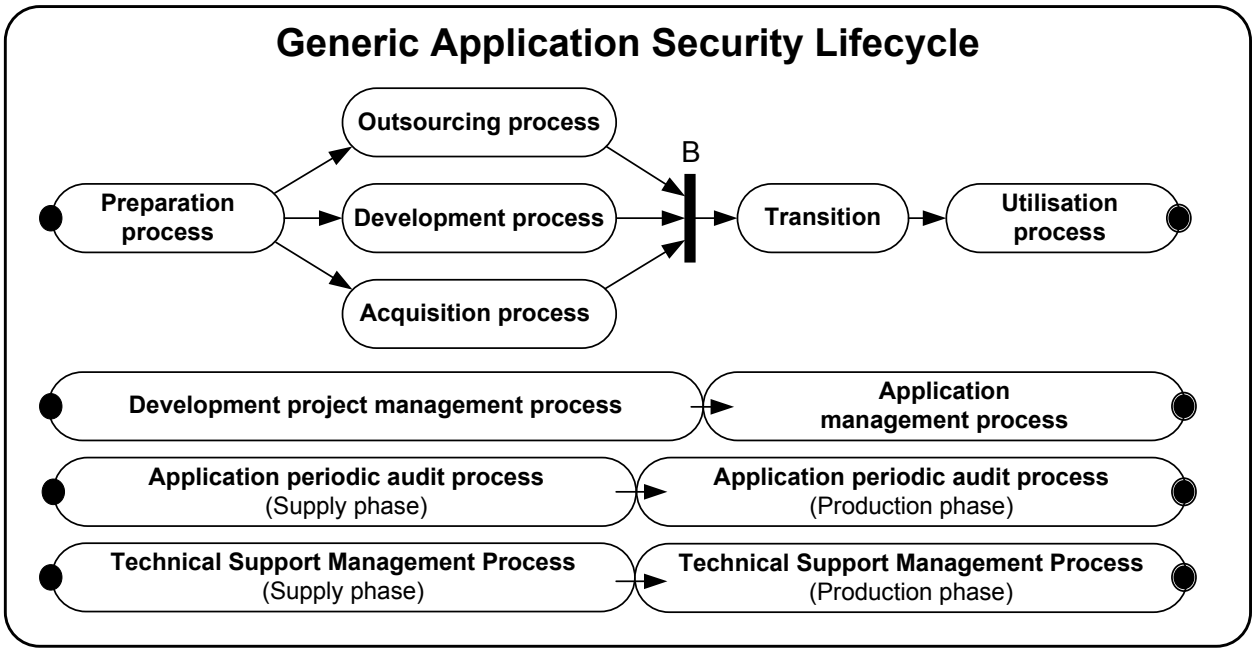

Figure 8 – Simplified view of the Generic Application Security Lifecycle

The organisation must then define a permanent mapping between the processes in this GASL and the processes already in use in the organisation’s own ASL. This will provide a way to indicate at which point in the organisation’s processes the ASMs will be applied.

The organisation’s ONF committee will determine the placement of ASMs in the GASL. This will ensure that application security is applied uniformly in all application projects in the organisation. Figure 9 shows the GASL in the ONF after ASMs have been attached to the various processes and roles.

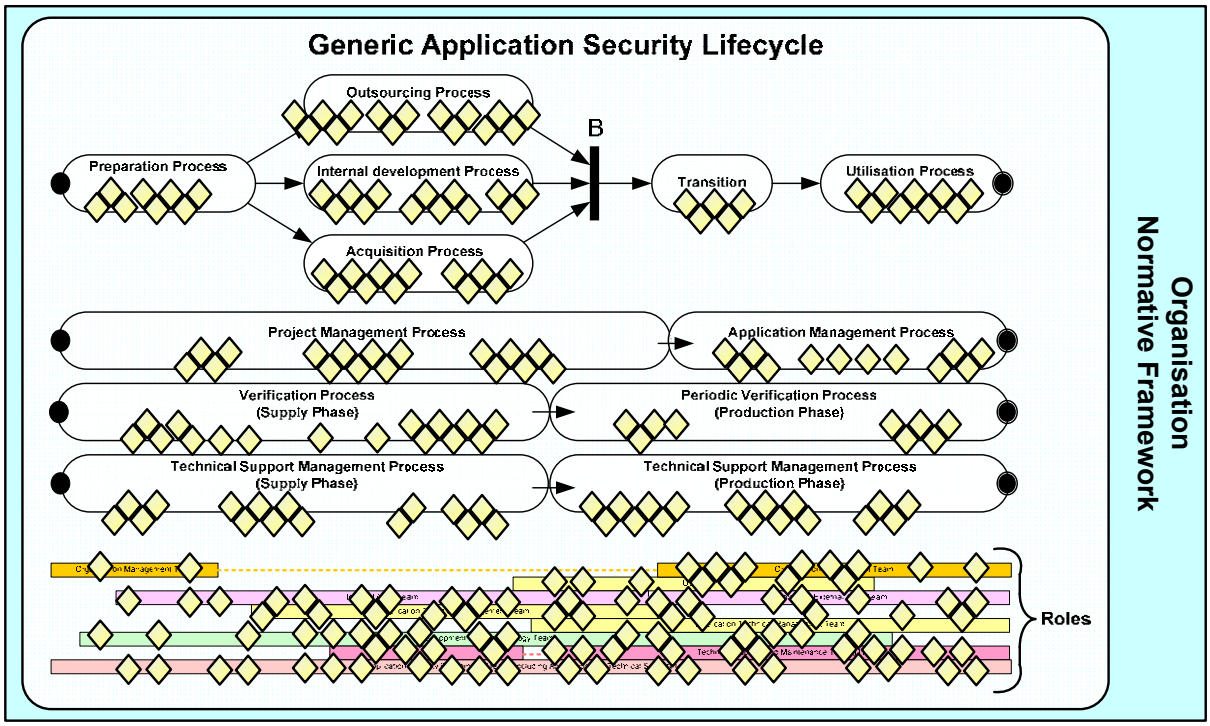

Figure 9 – Generic Application Security Lifecycle with ASMs attached

Roles are subjected to controls because the organisation must ensure that required qualifications are stated for each role, and that the principle of separation of duties is respected.

Processes included in the GASL are defined as follows.

6.1.7.1 Preparation Process

⇒ *To be completed.*

6.1.7.2 Outsourcing Process

⇒ *To be completed*

6.1.7.3 Internal Development Process

⇒ *To be completed.*

6.1.7.4 Acquisition Process

⇒ *To be completed.*

6.1.7.5 Transition Process

⇒ *To be completed.*

6.1.7.6 Utilisation Process

⇒ *To be completed.*

6.1.7.7 Project Management Process

⇒ *To be completed.*

6.1.7.8 Application Management Process

⇒ *Includes the change management process*

⇒ *To be completed.*

6.1.7.9 Verification Process – Supply Phase

⇒ *To be completed.*

6.1.7.10 Periodic Verification Process – Production Phase

⇒ *To be completed.*

6.1.7.11 Technical Support Management Process

⇒ *To be completed.*

6.1.8 Processes related to the Organisation Normative Framework

The ONF contains laws, standards, methodologies, policies, security design patterns, accepted coding standards and best practices recognized by the organization. These have to be kept up to date.

The organisation must define and document processes for creating, approving and maintaining the ONF and all of its components. Roles, responsibilities and required qualifications for these processes must be specified. For example, Figure 10 shows an overview of the ONF maintenance process.

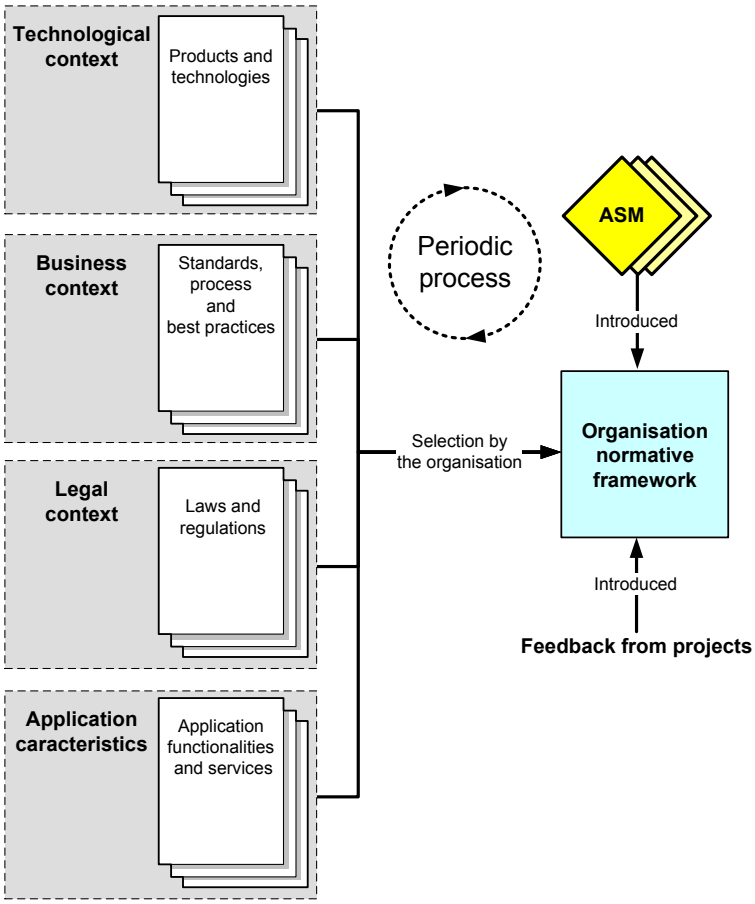

Figure 10 – Organisation Normative Framework maintenance process

Processes related to the ONF are permanent, organisation-level processes. They are independent from and performed in parallel to business application projects.

Processes must be defined for:

- ensuring that application security needs are still aligned with the organisation's business needs;
- securing high-management approval all organisation-level policies and other ONF components;

- ensuring the application security processes are adequately and uniformly applied organisation–wide;
- communicating the ONF components to all teams in the organisation;
- feeding back in the ONF any new knowledge and new good practices gained in the course of a business application project.

⇒ *Present the ONF implementation strategy for an organisation.*

⇒ *Present briefly (a few lines) two ONF implementation strategy examples, one for a small organisation (less then 10 developers) and one for a bigger organisation.*

6.2 Application Security Risk Management

6.2.1 Presentation

The second step of the ASMP involves the Application Security Risk Management (ASRM). A specific application-oriented risk analysis must be performed for each application. This process starts at the beginning of the application security lifecycle and will have an impact on different phases of the application's lifecycle. The main purpose for this step is to receive the organisation's approval on a targeted level of trust for the application, and periodically revise this target.

The ONF committee will identify the adequate ASRM process for the organisation's application projects and the ASMP will ensure that every project uses it correctly.

⇒ *Add reference to ISO 27005*

An organisation cannot develop or implement an application securely if it does not know what risk is involved in using this application. Figure 11 shows that this risk is determined by the application contexts and characteristics.

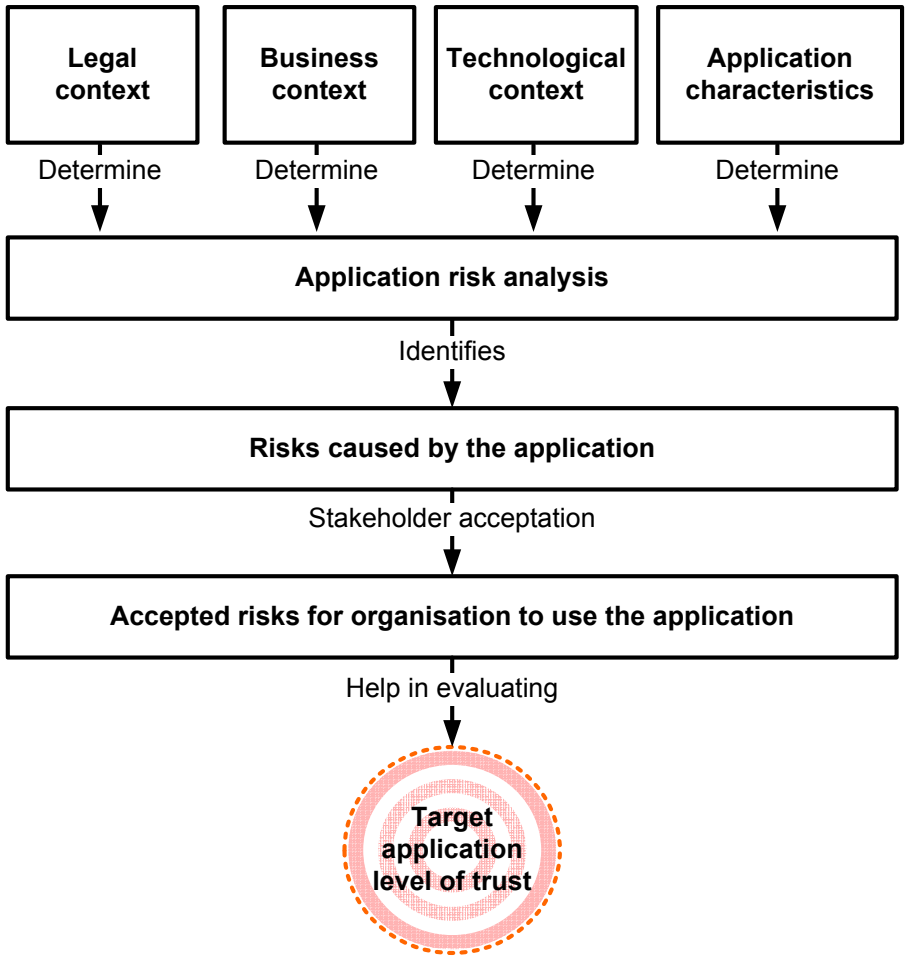

Figure 11 – Application security risk analysis process.

6.2.2 Components

6.2.3 Target application level of trust

A confidence level needed by the organisation that will use the application.

This must be one of (or within the range of) the levels of trust defined in the Organisation ASM Library, which is part of the ONF (see subclause 6.1.3).

The result of an application risk analysis that identifies risks brought by a planned business application, and a risk management process that determines the accepted risks. This then determines the application level of trust needed by the organisation and that will be targeted by the application project.

The target application level of trust is vital to the security of the business application because it directly determines the ASMs used in the project.

6.2.4 Impact of contexts and application characteristics on risks and application level of trust

⇒ *Explain how the different contexts and the application characteristics may have an impact on the targeted application level of trust. Show examples (technologies, business contexts, etc.)*

6.2.5 Processes

6.2.5.1 High-level application risk analysis

This is a high level risk analysis performed during the preparation phase of the application security lifecycle. It defines quickly as soon as possible the level of trust needed for a specific instance of an application according to its characteristics and contexts.

The organisation must perform this step using a risk analysis methodology adequate for an application-level analysis. An organisation-level risk analysis methodology is not designed for this task.

⇒ *This has to be further investigated. ISO 27005 defines ISMS risk analysis. It might be necessary to propose changes to ISO 27005 so that a more granular analysis can be applied to business applications.*

6.2.5.2 Detailed application risk analysis

This is performed during the internal development process of the application security life cycle. It defines more precisely the residual risks and confirms the level of trust needed for this specific application instance according to its detailed characteristics and contexts.

As a result of this process, the organisation may change the target level of trust for the application project. This may change the ASMs involved in the project. This in turn may change the actors involved and the cost of the project. However, those impacts are easily predicted since such information as actors, qualifications and cost are already part of each ASM.

The organisation must perform this step using a risk analysis methodology adequate for an application-level analysis. An organisation-level risk analysis methodology is not designed for this task.

⇒ *This has to be further investigated. ISO 27005 defines ISMS risk analysis. It might be necessary to propose changes to ISO 27005 so that a more granular analysis can be applied to business applications.*

6.2.5.3 Stakeholder acceptation

This is a risk management process in which the risks are analysed and stakeholders decide on the acceptable residual risks. This determines the target level of trust for the business application. Higher risks will result in a higher target level of trust.

6.3 Application Normative Framework

6.3.1 Presentation

The Application Normative Framework (ANF) is a subset of the ONF that will contain only the information required for a specific business application to reach the targeted level of trust.

The ONF already contains a generic ANF, a template for a minimal-level ANF (see subclause 6.1.6). For each application project, this template will be reused from the ONF, and completed with the relevant contexts, application characteristics and ASMs needed for the project.

The result will be an ANF customized for a specific business application project.

An ANF may evolve in time, during the application lifecycle. For example, the application legal context may change, or the organisation may re-evaluate the targeted application level of trust for an application. In theses cases, new elements may be added or removed from the ANF.

All ANF changes may have an impact on the application and must be addressed by the organisation as soon as possible.

A business application project must have a formal ANF, which must contain components from the ONF as detailed below.

6.3.2 Components

6.3.2.1 Application technological context

All technological components of the application such as: architecture, infrastructure, protocols, languages, etc.

6.3.2.2 Application business context

All processes, methodologies, standards and actors needed by the project, including processes outside the application but necessary to provide adequate integrity in real world terms.

6.3.2.3 Application legal context

Laws and regulations applicable in the location where the application will be used.

6.3.2.4 Application characteristics

⇒ *Functionality and process*

⇒ *Data (all application data including configuration data, parameters, users data, and the data used by the application)*

⇒ *Users (including end users, administrators, super-admin, DBA, technicians, pilots, etc.)*

⇒ *All the data used, stored, computed, shared or transferred by the application must be identified and categorised.*

⇒ *All output from the application in whatever form.*

6.3.2.5 Selected ASMs for the application project

A list of all ASMs selected for the application project.

This is the toolbox used by both the execution team and the verification team for securing the application. Each ASM provides a security activity and a control, along with pointers to specific phases in the application lifecycle processes where said activity and control will be performed.

6.3.3 Application Security Lifecycle

The Application Security Lifecycle (ASL) is the name given in this standard to the collection of processes (development process/methodology, acquisition process, change management process, etc) already in use in the organisation. It presents a process-oriented view of application security activity and controls.

The ASL and its standard counterpart the Generic Application Security Lifecycle (GASL) have already been discussed in subclause 6.1.7.

The Application Security Measures (ASMs) contained in the ANF will point to various phases of the processes in the organisation's ASL as a way to indicate "when" security activities and controls must be performed.

The execution team and the verification team are already familiar with those phases and processes.

⇒ *As a reference, ISO 12207 defines a list of processes that may be included in the organisation's ASL.*

⇒ *We will check ISO 12207 later and see how this can be referenced or integrated.*

6.3.4 Processes

6.3.4.1 Processes related to the Application Normative Framework

The organisation must define and document processes for creating, approving and maintaining the ANF. Roles, responsibilities and required qualifications must be specified.

The ANF creation process is vital. This process will transform generic information contained in the ONF into specific information in the ANF.

ASMs in the ONF are linked to phases of the Generic Application Security Lifecyle. This is not directly useful to the project execution team because the organisation uses its own lifecycle that is different from the generic one.

Subclause 6.1.7 states that there must be a permanent mapping between the processes in the GASL and the processes in the lifecycle already in use in the organisation.

The ANF creation process will perform the transformation from generic to specific according to this mapping. The result will be a set of ASMs directly useful to the execution team because the ASMs will contain only information specific to the project.

For example, an organisation may have adopted the lifecycle defined in ISO 12207.

For this organisation, the development process in the GASL will be mapped with the ISO 12207 development process. In that way, the ASMs will be correctly placed on the ISO 12207 process timeframe and the ISO 12207 actors will be correctly associated with the actors identified in the GASL.

6.3.4.2 Feedback process

The organisation must define a process for continuously improving the ONF by feedback from every application project in the form of new or improved components such as ASMs, best practices, etc.

This process is shown on Figure 1 as “Produce new practices”.

This process must tie in with an ONF maintenance process shown in Figure 10 as “Feedback from projects”.

6.4 Business Application Project

6.4.1 Presentation

This step involves the actual use in the business application project of the Application Security Measures provided by the Application Normative Framework.

Each ASM contains both a security activity and a control, along with detailed information needed for performing the activity at a specific moment.

The execution team will implement all the security activities contained in all the ASMs contained in the ANF.

Project managers will find the ASM an efficient tool because it details the required tasks, the needed resources and their qualifications, the cost in days-person for the tasks and the exact point in the lifecycle at which the tasks must be performed.

The test team will find the ASM an efficient tool because it provides detailed information about what controls will be performed by the verification team at the end of the project. This allows the test team to make sure the business application meets the security requirements before delivery.

The security team and the technology team will find the ASMs useful because they provide a list of all security requirements, thus allowing advance planning needed resources.

6.4.2 Components

6.4.2.1 Execution Team

⇒ *Describe and detail the execution team*

⇒ *Present the ASL actors and main qualifications and responsibilities of the execution team versus the targeted level of trust.*

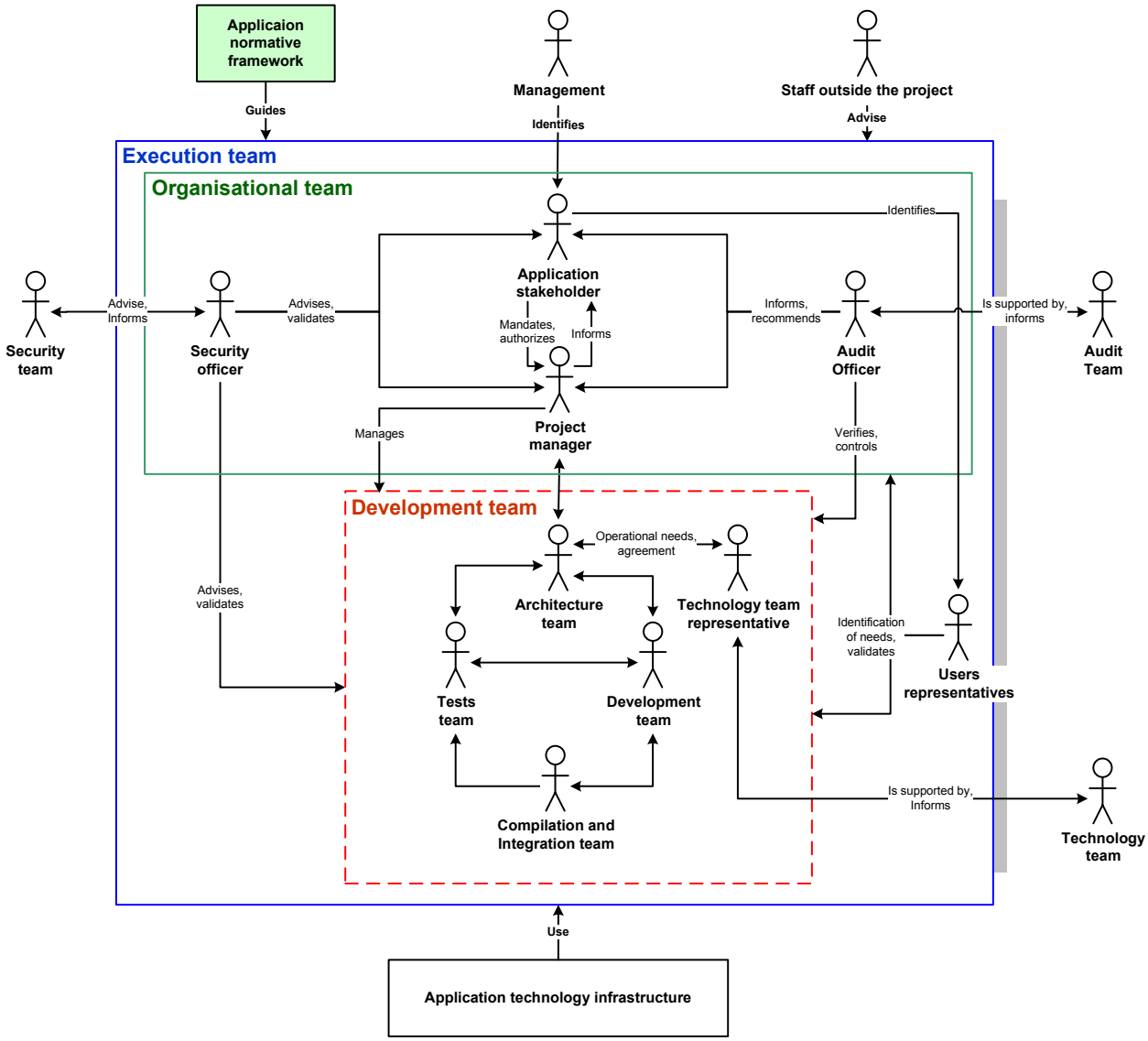

Figure 12 –Roles in the execution team

6.4.3 Processes

6.4.3.1 Performing security activities in the course of a business application project

Figure 13 shows how the execution team uses the ASM as a tool for performing security activities.

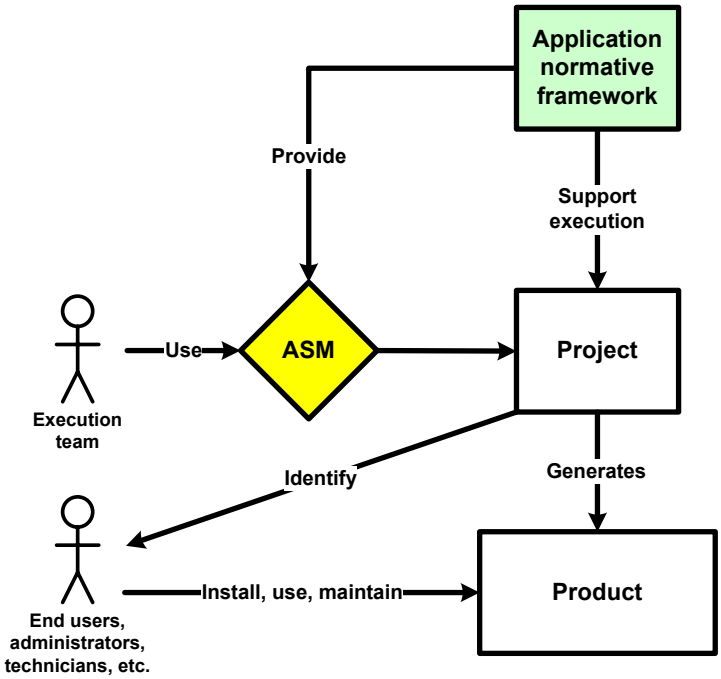

Figure 13 – ASM used as a security measure

6.5 Application Security Verification

6.5.1 Presentation

In this step an internal or an external verification team (depending on organisational policies contained in the ONF) will perform all the controls provided by the ASMs in the Application Normative Framework.

The audit (verification) team and the security team will find the ASM useful because it provides detailed information on the security activity and related control. Control procedures and expected results are provided.

Project managers will find the ASM an efficient tool because it details the required tasks, the needed resources and their qualifications, the cost in days-person for the controls and the exact point in the lifecycle at which the controls must be performed.

The purpose of this step is to verify and provide hard evidence that an application has reached and maintained the targeted level of trust. It will measure the actual application level of trust at a specific time. Depending of the level of trust needed for the particular application project, this process may be unique, periodic, or event-driven.

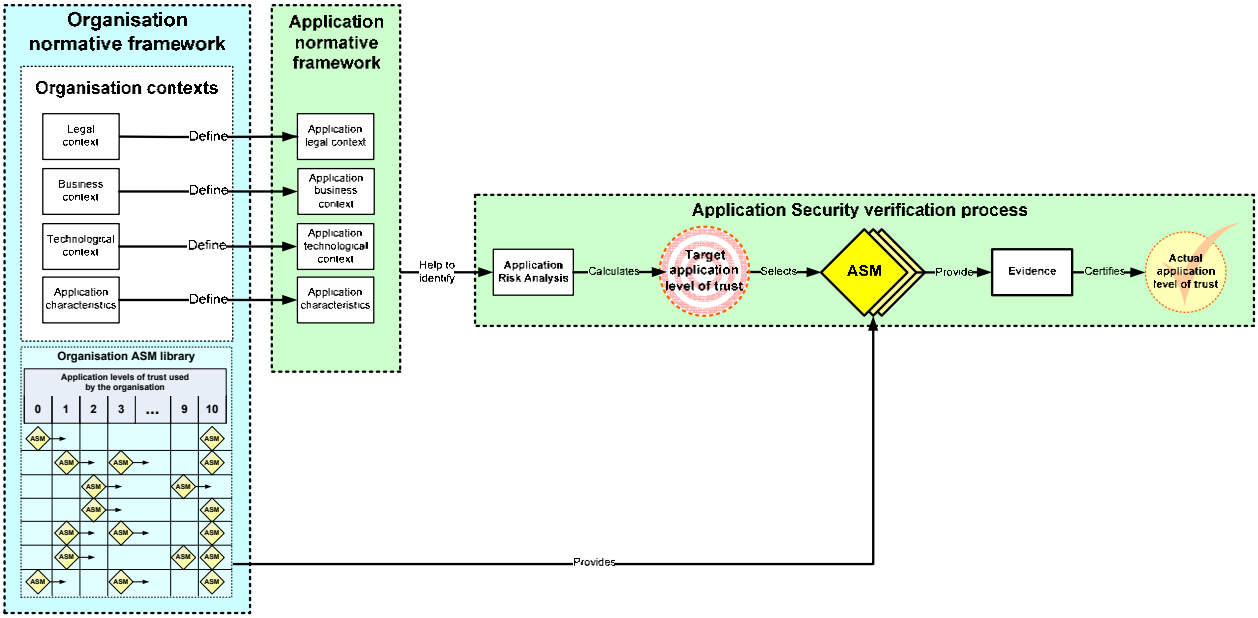

Figure 14 – Application security verification process

⇒ *Present and describe all input, processes and output involved on the different controls.*

6.5.2 Components

6.5.3 Actual application level of trust

The measured security confidence level for the application.

Every ASM included in the ANF for any given application project provides a specific and detailed control to be performed by the verification team, along with a pointer to the specific moment in the ASL the control must be performed.

The level of trust of an application is confirmed when the successful verification of all ASMs identified by the targeted level of trust has been performed. At this moment, it is considered secure for an organisation to use this application, for a specific period of time.

Figure 6 shows how the verification team uses the ASM as a control.

⇒ *Present and describe the elements of the figure*

⇒ *Explain that application security may have to verify and control the ONF, the project processes, the product itself, and the people (actors) who participate to the project, will use or are using the product.*

Annex A (informative)

Application Security Management Process – Case Study

⇒ *This part is not mature and needs discussion in Kyoto. Industry input might be needed.*

⇒ *This annex will present a case study of application security implementation on an application projects*

⇒ *It will clearly present, using examples, the process to ensure that only those ASMs selected for a specific application will be used to measure the actual application level of trust.*

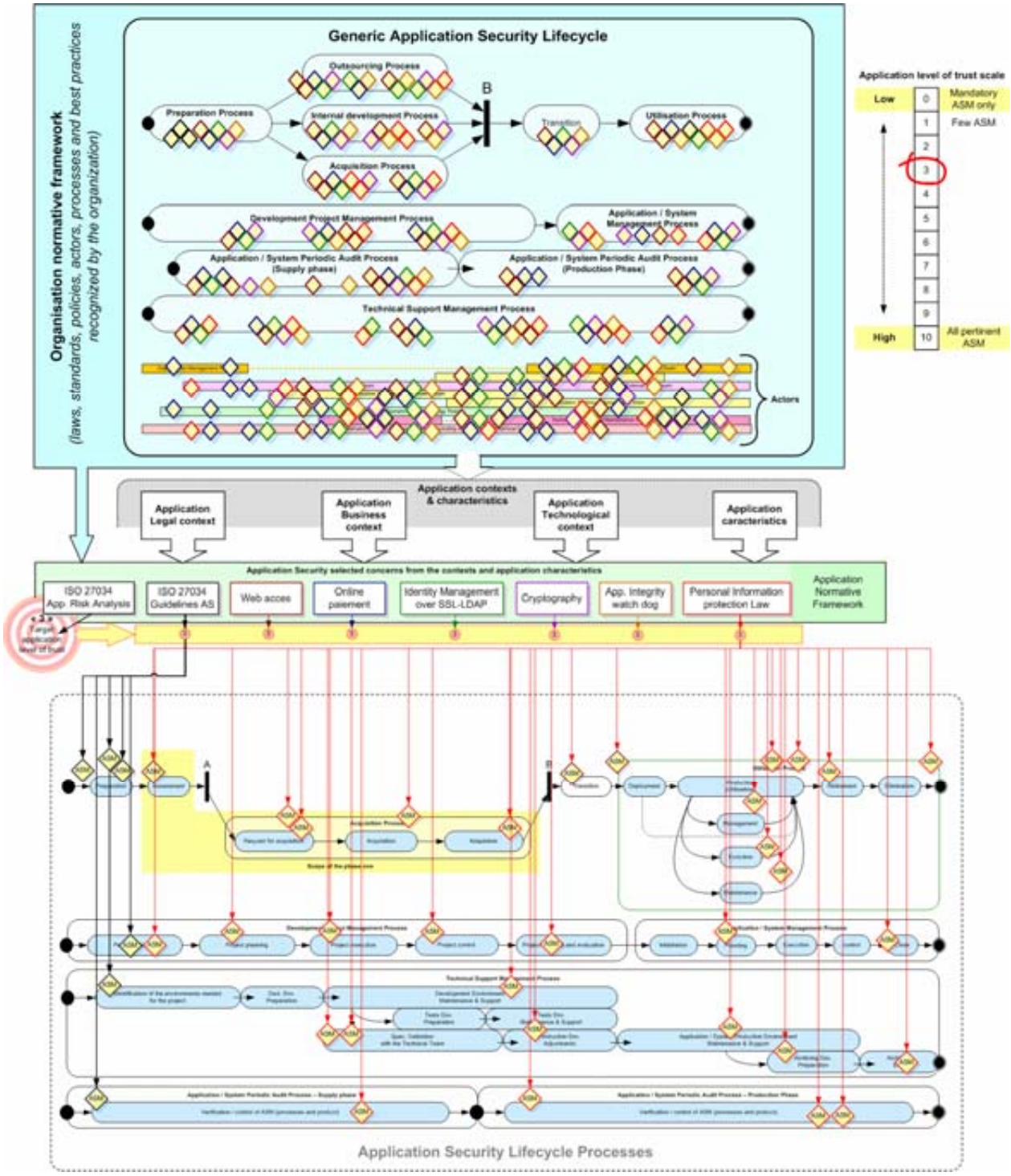

Figure 15 – Possible visual depiction of a ASMP Case Study

⇒ *This section will present a quick checklist to obtain application security. This checklist will have to be adapted to an organisation's business priorities.*

⇒ *Checklist example (to be completed):*

1) Develop the first version of your ONF

a) Identify the laws and regulations that can impact your organisation through the application

b) Identify the technologies used or that can impact the application availability, or have an impact on data integrity and confidentiality

c) Identify the business process and operations that can be impacted by your application

d) Identify the people (actors and users) who have to interact with the application and precise their roles, responsibilities and minimal qualifications.

e) To be completed.

2) For each element defined in step 1, identify the most important ASMs that can be easily defined at this point, to start your application security improvement and verification.

Note: The ASM is the tool to insure the introduction of the right application level of trust with two strategies:

i) by inserting ASMs in all processes on the application life cycle to verify the processes themselves and the people who are part of it.

ii) by defining an ASM tree concerning security requirements, functionalities and characteristics for an application, to verify the application itself.

b) Fill the ASM template with the correct information.

i) Write the header, the objectives, the activity and the control processes that have to be performed when this ASM will be involved.

ii) The relevant ASMs from the right level of trust of an application must be validated on every cycle of its system lifecycle, as requested.

c) Associate each ASM to one level of trust. . This ASM will have to be used every time this level of trust will be targeted by the organisation for an application.

d) Require management approbation for the organisation ASM library

e) To be completed.

3) An application that passed the certification of all its ASMs is considered secure at its actual level of trust, at this precise moment.

⇒ To be completed.

Annex B
Acronyms

ANF	Application Normative Framework
ASC	Application Security Certification
ASL	Application Security Lifecycle
ASM	Application Security Measure
ASMP	Application Security Management process
ASRM	Application Security Risk Management
COTS	Commercial-Off-The-Shelf Product
GASL	Generic Application Security Lifecycle
ISMS	Information Security Management System
ONF	Organisation Normative Framework

Bibliography

⇒ *To be completed.*