B ISO 27034

Main Reference *ISO/IEC 27034-1:2014: Information Technology – Security Techniques – Application Security*.

This appendix provides an overall view of the ISO27034 standard in its current state. It only parses the main concepts and elements that this standard provides. Some parts are closely related perhaps sometimes very similar to these of the standard. Note that the figures presented in this appendix all come “as is" from the main reference.

B.1 Introduction

The purpose of this document is to facilitate application security integration for the organizations by providing concepts, principles, procedures, mechanisms and security controls that allow to provide evidences that their applications reach a certain degree of security.

The main principles of this standard are the followings :

- *Security is a requirement* : this is necessary and should be addressed in any process.
- *Application security is context-dependent* : that is, security has to deal with different risks according to specific contexts, especially as defined in the standard, *business*, *regulatory* and *technological* contexts.
- *Appropriate investment for application security* : The costs of assessments should be seen as an investment as they allow to spare other costs due to consequences of security breaches.
- *Application security should be demonstrated* : The audit process should lead to verifiable facts through security controls.

Figure B.1 shows the relationships between ISO 27034 and other ISO standards. One can point out three parts in this figure :

1. Sources of security controls (the four leftmost boxes) : These encompass standards addressing criteria, models, codes of practices and techniques that can be consulted for building the elements of the framework defined in ISO27034.
2. Processes and activities (the two downmost boxes) : ISO27034 provides definitions of useful processes and activities that can be used to control life cycles, either for software or systems.

3. Support to higher-level standards (the four rightmost boxes) : ISO27034 provides helpers for the implementation of management and assurance standards.

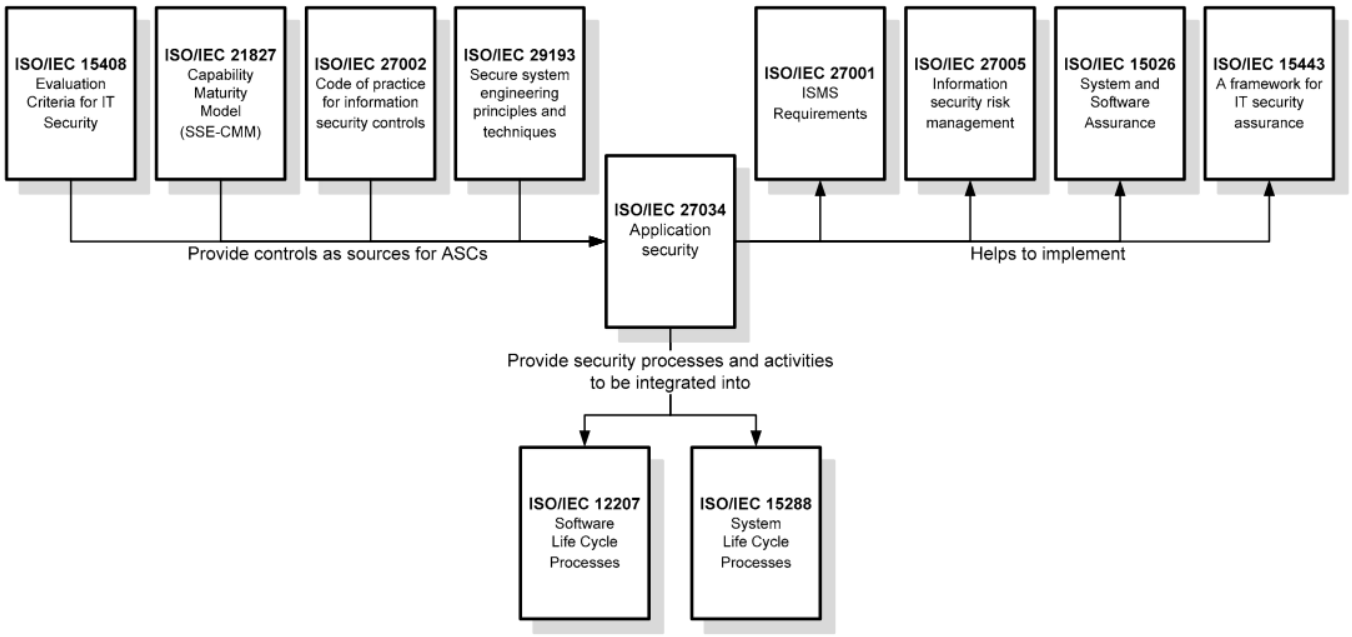

Figure B.1: Relationship to other International Standards

B.2 Overview

This section presents how ISO27034 is structured and its current state and then the most important concepts of its framework.

B.2.1 Structure

This standard is structured in seven parts :

ISO/IEC 27034-1:2011 – Overview and concepts

ISO/IEC 27034-2:2015 – Organization normative framework

ISO/IEC 27034-3 – Application security management process (draft)

ISO/IEC 27034-4 – Application security validation (cancelled)

ISO/IEC 27034-5 – Protocols and application security control data structure (draft)

ISO/IEC 27034-6 – Case studies (draft)

ISO/IEC 27034-7 – Application security assurance prediction (draft)

As one can point out, this standard is still in its early stage. ISO27034-1:2011 was reviewed and now published as ISO27034-1:2014. Both already published parts define the framework and its concepts and elements. ISO27034-3 and ISO27034-5 should provide in the future the last details for allowing the full implementation of the standard in organizations. ISO27034-6 should also provide very useful information for helping to the implementation.

B.2.2 Main Concepts

This standard essentially relies on the following concepts :

- **Actual Level of Trust** : This is a metric providing the level of assurance that the framework is correctly implemented and applied. This is the result of the whole process.
- **Application Security Control (ASC)** : This is the raw material of the framework. This is a data structure holding attributes such as an identifier, a description and the measurement it addresses.
- **Organization Normative Framework (ONF)** : This is a structure consisting of the normative application security processes and elements for the whole organization.
- **Application Normative Framework (ANF)** : This is a subset of ONF, applied to a specific application.
- **ASC Library** : This is the library of all ASC defined by the organization. When instantiating an ANF, the ASC library is where the pieces of the implementation are taken.

B.2.3 Organization Normative Framework (ONF)

The ONF is like a storage for all best practices about application security. It consists of what is named in a general way components. These encompass the contexts (business, regulatory and technological), specifications, roles (and responsibilities), processes (and sub-processes), models and the ASC library (see Subsection B.2.4). A representation of the ONF is depicted in Figure B.2.

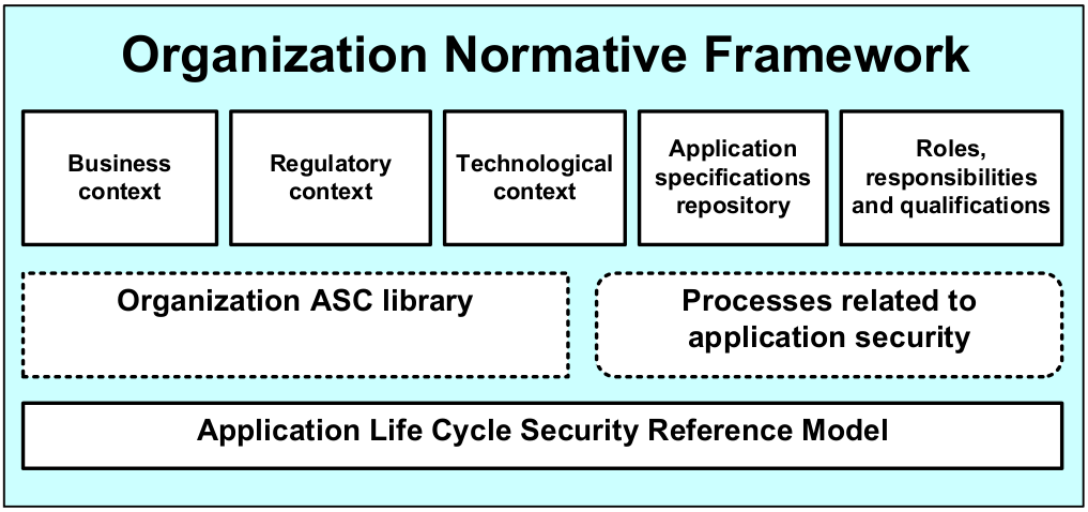

Figure B.2: Organization Normative Framework (simplified)

Regarding the contexts :

- **Business** : This gathers the documentation on standards and best practices impacting the applications. It includes organization's processes about everything relating to applications (management of project, development, risk, audit, ...) and the general security policy.
- **Regulatory** : This concerns any law or regulation applicable to the whole or any part of the organization.
- **Technological** : This consists of the documentation of all available technologies in the organization, either for business objectives or for implementing security controls.

B.2.4 ASC Libary

This library gathers all ASC's defined by the organization from any component of the ONF. ASC's are themselves gathered into sets corresponding to a specific level of trust. Note that such a level is just a shortcut aimed to facilitate the communication regarding the sets of ASC's. The following example in Figure B.3 illustrates this.

EXAMPLE

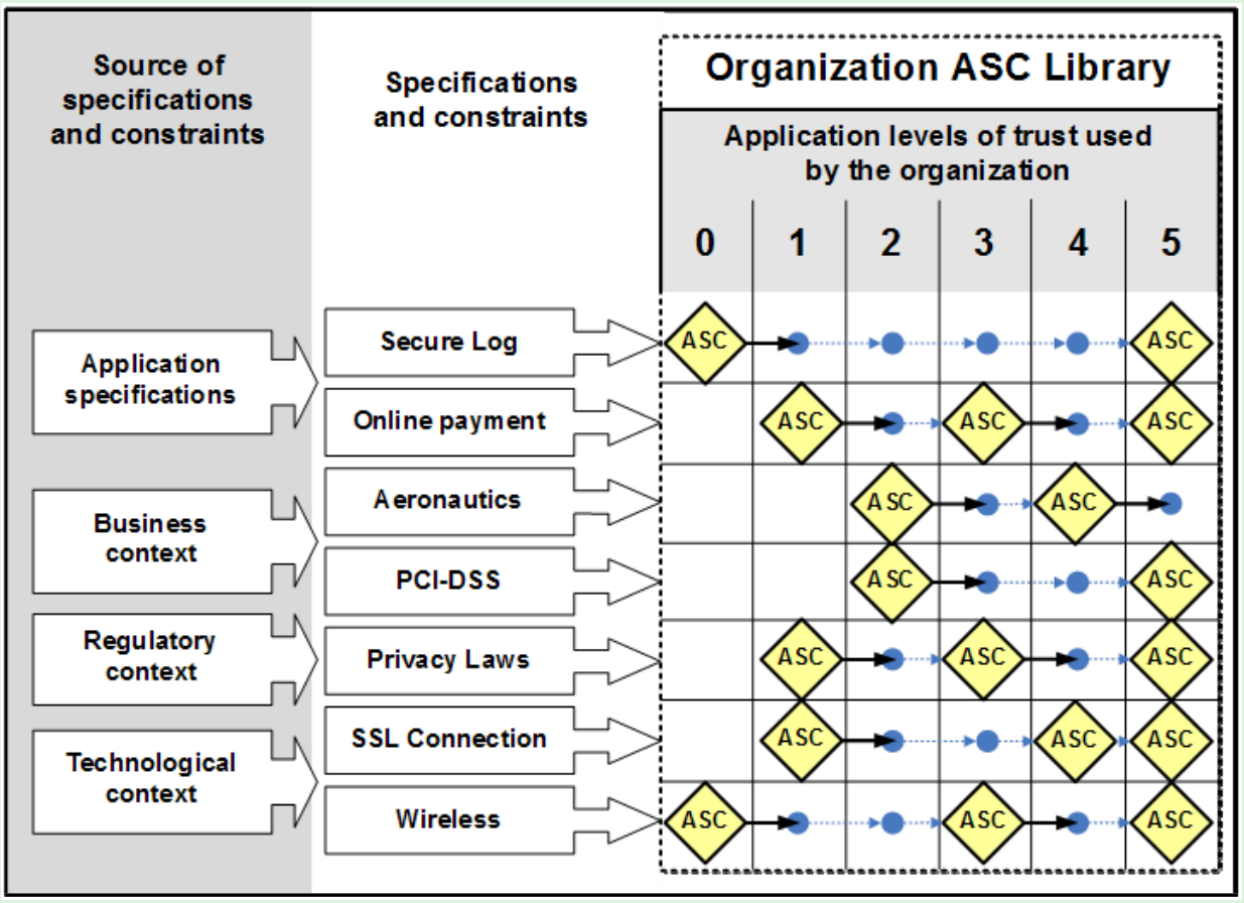

Figure B.3: Example of ASC library

In this example, one can see in a first phase the contexts used as sources of specifications. In a second phase, specifications are deduced and the ASC's can then be defined and ranked according to the defined levels of trust.

In the library, ASC's have various purposes :

- Securing application components (files, data and infrastructure)
- Security activities (for processes)
- Verification of roles and responsibilities
- Determination of acceptance criteria
- Determination of Actual Level of Trust

The components of an ASC are represented in Figure B.4. These components can be considered as attributes of the data structure of the ASC. They must answer all important questions that make the ASC consistent, that is, the *why*, *what*, *how*, *where*, *who*, *when* and *how much*. Other attributes complete the definition such as the identification, the author, the objective and so forth. The formal definition of the ASC should be addressed in ISO27034-5 in a near future.

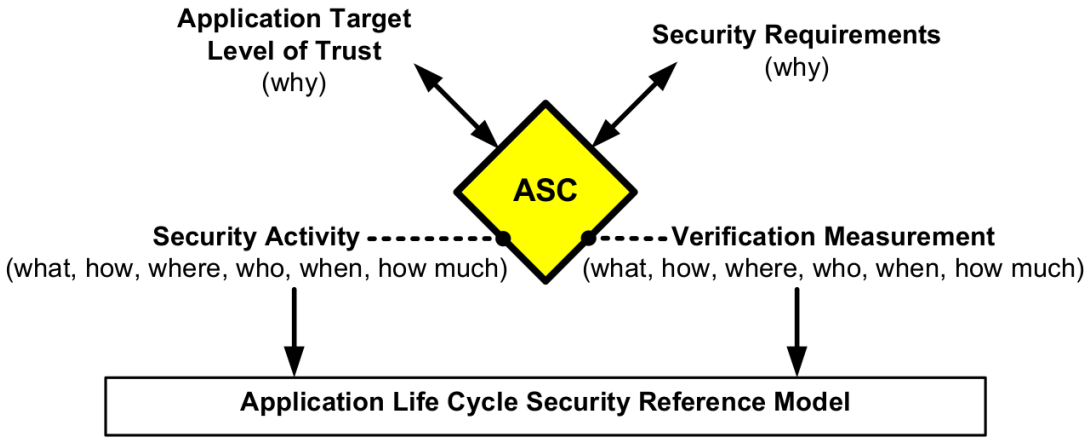

Figure B.4: Components of an ASC

B.2.5 Application Normative Framework (ANF)

The ANF is defined as a subset of the ONF, gathering only the necessary information related to the application on which the organization wants to reach a certain level of trust. A representation of the ANF, very similar to this of the ONF of course, is depicted in Figure B.5.

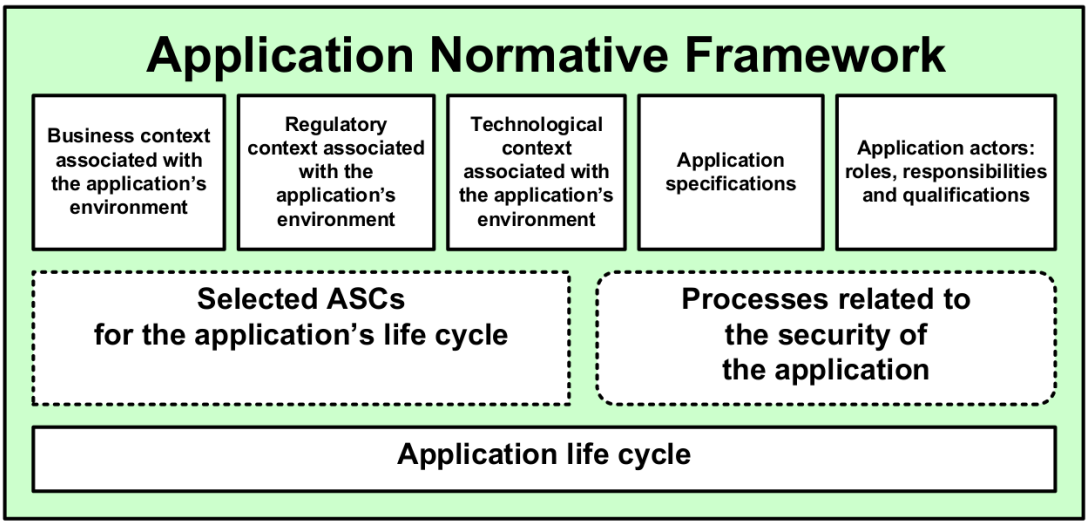

Figure B.5: Application Normative Framework

The box *Processes related to the security of the application* encompasses all processes defined to manage and verify the application security such as risk assessment, vulnerability assessment, ...

B.3 Processes

Beyond the concepts and principles, ISO27034-1 also provides a few processes to manage the components.

B.3.1 Organization Management

This set of processes allow to manage the ONF as well as its instances, the ANF's. The relationships between these processes are depicted in Figure B.6.

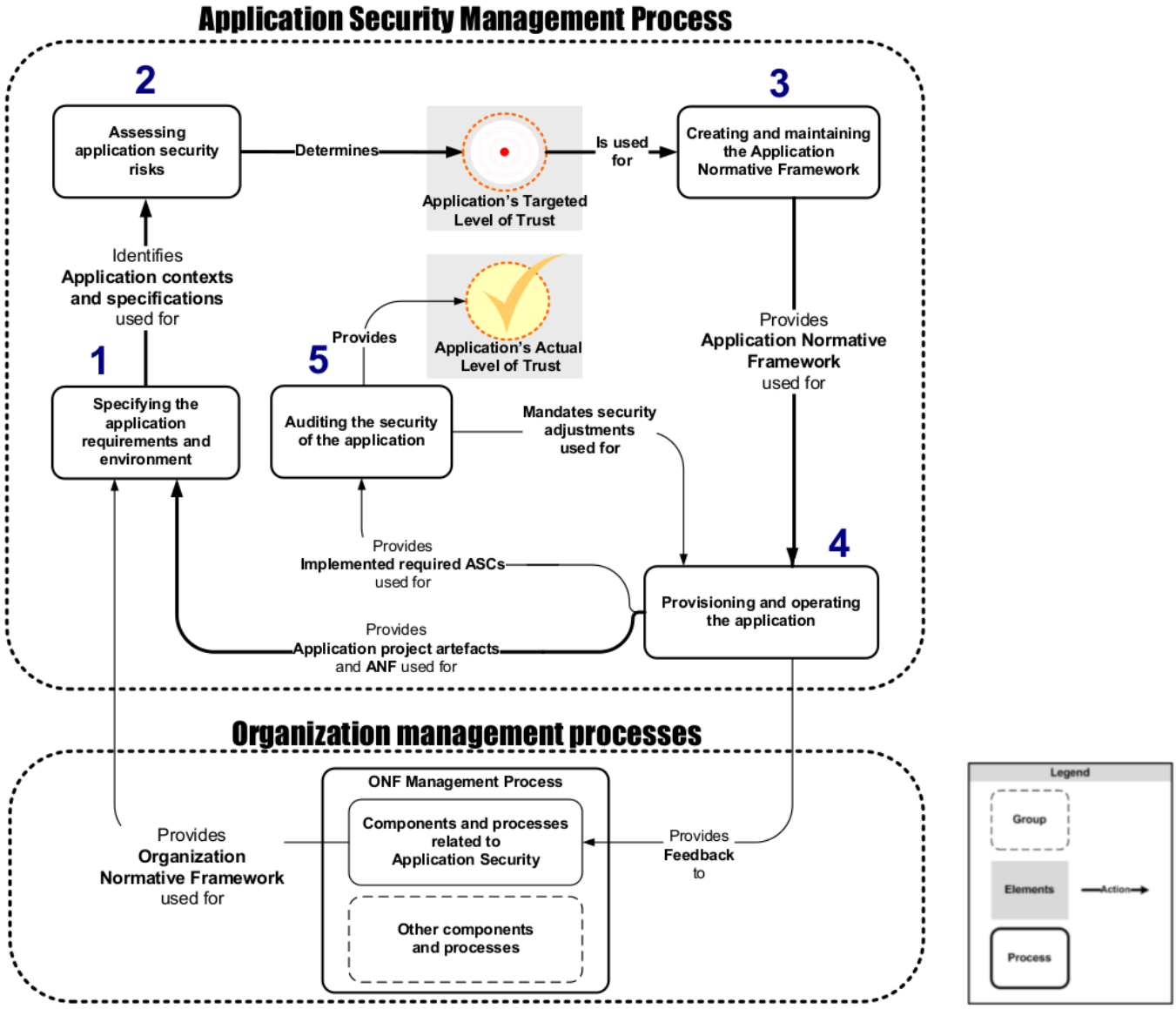

Figure B.6: Organization Management Processes

This figure shows two main processes :

1. **ONG Management Process** : This encompasses all sub-processes related to the application security, including all components of the ONF.
2. **Application Security Management Process** : This five-steps process resumes all necessary activities in order to make an application compliant with a certain level of trust, including specifications, ANF definition, provisioning, testing and assessment of the application.

B.3.2 Application Security Verification

In the scope of Application Security Audit, that is, step 5 of the Application Security Management Process in Figure B.6, ISO27034-1 also defines a process for security verification. This process is depicted in Figure B.7.

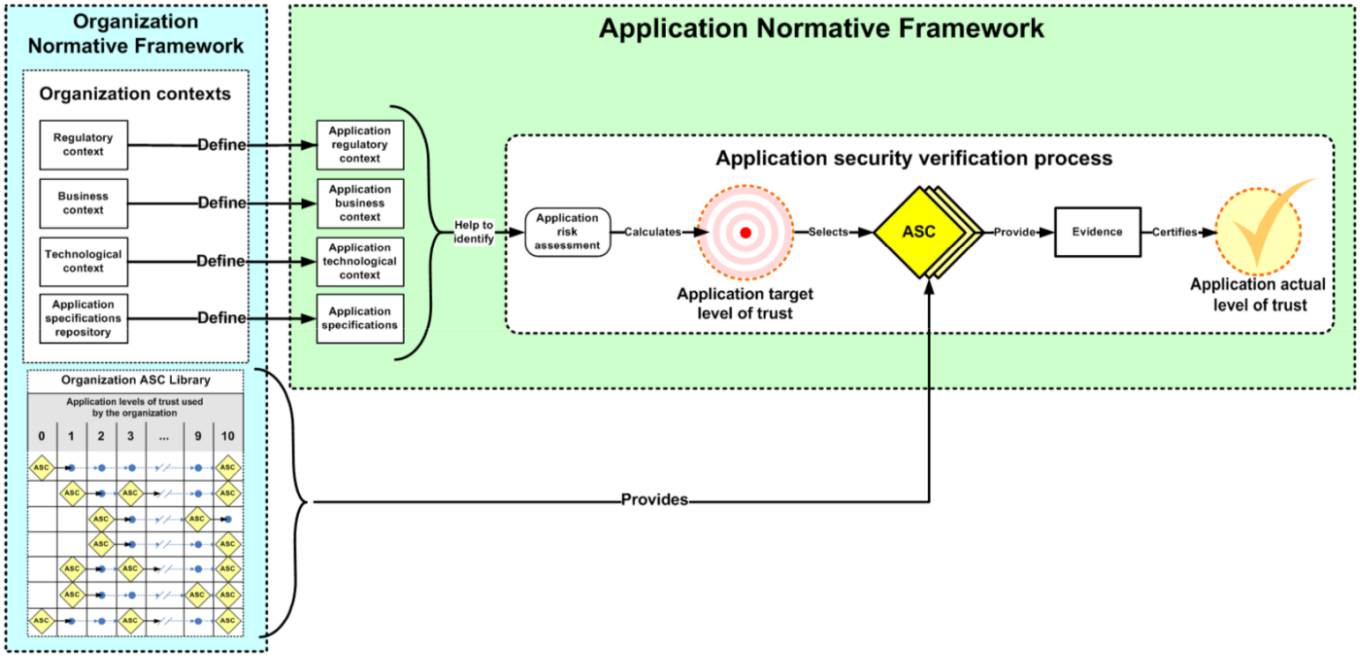

Figure B.7: Application Security Verification Process

This process starts with a risk assessment based on the documentation from the ONF (contexts and specifications) so that a targeted level of trust can be defined. The relevant set of ASC, that is the ANF, is then extracted from the ASC library in order to perform related measurements that lead to the determination of the actual level of trust, which is the final output that confirms that the application is secure.

B.4 Relationship with NIST SP 800-53

ISO27034-1 provides an excellent appendix making a mapping between security controls from NIST SP 800-53 Rev3 to ASC's. In essence, the work method is to take the classes and sub-classes of security controls from the Appendix of the NIST standard and to parse them for candidate ASC's. The Appendix B of ISO27034-1 performs this job for the *Access Control* class from NIST SP 800-53 Rev3.