INTERNATIONAL STANDARD

ISO/IEC 27034-7

First edition
2018-05

Information technology — Application security —

Part 7: **Assurance prediction framework**

Technologies de l'information — Sécurité des applications —

Partie 7: Cadre de l'assurance d'une prédiction

Reference number
ISO/IEC 27034-7:2018(E)

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

Published in Switzerland

Contents

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 document 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 and IEC 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, *Security techniques*.

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

0 Introduction

0.1 Basic prediction

The project team declares an application secure when the supporting evidence demonstrates the attainment of the Targeted Level of Trust (ISO/IEC 27034-1:2011, 0.4.4). A security prediction occurs when the project team uses the supporting evidence from a previous version of the application and provides a rationale as to why the supporting evidence is still valid for the subsequent application. The security prediction framework is the process whereby organizations, who use ISO/IEC 27034 (all parts), perform risk analysis and document decisions made, relative to Application Security Controls (ASCs) performed on a previous version of an application but not performed on the current version. All such predictions are fundamentally subjective, and at best can only express a degree of confidence.

Today, individuals and organizations already transfer their confidence in security claims between versions of applications without any strong rationale supporting this transfer. Making a security prediction for a subsequent application, without any rationale or justification, is inherently a bad practice. To rectify this situation, this document establishes a framework by codifying requirements for making security predictions between versions of an application.

This document focuses on predictions, or claim transfers, related to subsequent versions of the same application.

0.2 Purpose

The purpose of this document is to help organizations to develop and use Prediction Application Security Rationales (PASR) in disseminating information relative to security properties of multiple versions of the same application by:

a) providing additional guidance to Organization Normative Framework (ONF) Committees so that they can set up appropriate guidelines for when predictions are and are not appropriate for their organizations;

b) providing the results of a risk analysis that contains the rationale as to why the changes in the subsequent application are not substantial;

c) applying to application projects that are using an Application Normative Framework (ANF);

d) indicating the Actual Level of Trust for the original and subsequent applications;

e) indicating the Expected Level of Trust for the original, if used, and subsequent applications;

f) providing the rationale as to why the risk analysis, predictions for individual Application Security Control (ASC), and the Actual Level of Trust together produce the Expected Level of Trust; and

g) verifying a PASR when the auditor chooses to rerun the corresponding ASC verification activity.

This document does not provide guidelines on:

a) what is and is not an appropriate risk;

b) what is and is not substantial change;

c) when an application owner should or should not accept a specific risk; or

d) when an acquirer should or should not accept an Expected Level of Trust.

0.3 Targeted audience

0.3.1 General

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

a) managers;

b) ONF Committees;

c) project teams;

d) domain experts;

e) auditors;

f) application owners; and

g) acquirers.

0.3.2 Managers

The manager roles are the same as in ISO/IEC 27034-1:2011, 0.3.2.

0.3.3 ONF Committee

As described in ISO/IEC 27034-1:2011, 3.17, 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) provides guidelines to project teams as to what is and is not a substantial change;

b) evaluates, and documents, in the ASC, the risk of choosing the PASR over performing the ASC activity;

c) reviews each ASC and determines if predictions are allowed and, if allowed, under what circumstances predictions are appropriate;

d) documents the prediction determination in each ASC in the ONF;

e) advises the application owner, when establishing the ANF, the estimated risk of using the PASR; and

f) responds to requests from project teams to modify the prediction guidelines for specific ASC.

0.3.4 Provisioning and operation team

As described in ISO/IEC 27034-1:2011, 0.3.3, members of provisioning and operation teams (known collectively as the project team) are individuals involved in an application’s design, development and maintenance throughout its whole life cycle. The project manager is responsible for managing the ANF.

The project team:

a) performs a risk analysis on the proposed changes to the application to determine if the changes are substantial;

b) creates the PASR (as defined in 3.2) for each ASC for which there is a prediction; and

c) generates the Expected Level of Trust report.

0.3.5 Domain experts

An individual who is an expert in a particular domain, area, or topic that provides specific knowledge or expertise to the project team. These experts:

a) assist the project team in making an accurate risk assessment; and

b) assist the project team in making the determination if the changes to the application represent a substantial change.

0.3.6 Auditors

As described in ISO/IEC 27034-1:2011, 0.3.6, auditors are personnel performing roles in the audit process who participate in application verification.

0.3.7 Application owners

Based on the definition in ISO/IEC 27034-1:2011, 3.6, the application owner is the organization’s representative who is responsible and accountable for the security and the protection of an application. Application owners make the final decisions on:

a) acceptance of the project team risk analysis that the changes to the application are not substantial;

b) approval of a set of ASCs for which the project team generates PASRs; and

c) acceptance of the Expected Level of Trust.

0.3.8 Acquirers

This includes all individuals involved in acquiring a product or service. Acquirers:

a) perform actions as per ISO/IEC 27034-1:2011, 0.3.4;

b) evaluate if the Actual Level of Trust for the original application is appropriate to mitigate the risks the acquirer anticipates for the expected contexts the acquirer will use the application in;

c) evaluate if the Expected Level of Trust for the subsequent application is appropriate to mitigate the risks the acquirer anticipates for the expected contexts the acquirer will use the application in; and

d) evaluate if the rationale that changes to the subsequent application are not substantial and, if not in agreement with the rationale, determine if additional verification is necessary.

Information technology — Application security —

Part 7: Assurance prediction framework

1 Scope

This document describes the minimum requirements when the required activities specified by an Application Security Control (ASC) are replaced with a Prediction Application Security Rationale (PASR). The ASC mapped to a PASR define the Expected Level of Trust for a subsequent application. In the context of an Expected Level of Trust, there is always an original application where the project team performed the activities of the indicated ASC to achieve an Actual Level of Trust.

The use of Prediction Application Security Rationales (PASRs), defined by this document, is applicable to project teams which have a defined Application Normative Framework (ANF) and an original application with an Actual Level of Trust.

Predictions relative to aggregation of multiple components or the history of the developer in relation to other applications is outside the scope of this document.

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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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 27000, 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 https://www.iso.org/obp

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

3.1
prediction
statement or estimate that a specific thing will happen in the future or will be a consequence of something

Note 1 to entry: The origin of the word is early 17th century: from Latin praedict-“made known beforehand, declared”, from the verb praedicere from prae-“beforehand” + dicere “say”.

Note 2 to entry: The use in this document reflects the expectation that, if the security and verification measurement activities are executed, they will match the results from the original application.

3.2
prediction framework
process that performs a risk analysis, establishes an *Expected Level of Trust* (3.8), assigns Application Security Control verification to a *PASR* (3.7), and then creates an *Expected Level of Trust Report* (3.9)

3.3
original application
application that establishes the baseline Actual Level of Trust

Note 1 to entry: The original application is not necessarily version 1.0 and, hence, can have an associated Expected Level of Trust.

3.4
subsequent application
application related to the *original application* (3.3) through versioning

EXAMPLE Version 1 to version 1.1.

3.5
predictive security
transfer of confidence in the *security claims* (3.6) of the *original application* (3.3) to the security claims of the *subsequent application* (3.4)

3.6
security claim
specific claim that security properties are present in an application

Note 1 to entry: Under the ISO/IEC 27034 frameworks (all parts), it is the claim that the activities specified by an Application Security Control mitigate specific security risks to an acceptable level.

Note 2 to entry: In the context of a PASR, it is the claim that verification of the Application Security Control activities, which were predicted by the PASR, would produce the same results as if the Application Security Control activities were performed.

3.7
Prediction Application Security Rationale
PASR
rationale for a *prediction* (3.1), supported by risk analysis documents, approved by the application owner, explaining that performing the verification activities of a specific Application Security Control is not necessary

Note 1 to entry: Use of PASR requires approval of both application owner and the inclusion of the PASR guidelines in the Application Security Control by the Organization Normative Framework Committee.

3.8
Expected Level of Trust
level of trust, defined in the Organization Normative Framework, where the activities of some of the Application Security Controls are satisfied through the creation of a *PASR* (3.7)

Note 1 to entry: This document describes the minimum requirements applicable to the Application Security Controls used in an Expected Level of Trust for a *subsequent application* (3.4). In the context of an Expected Level of Trust, there is always an *original application* (3.3) where the project team performed the activities of the indicated Application Security Controls.

3.9
Expected Level of Trust Report
document presenting and supporting the risk analysis in support of *predictions* (3.1) made for a subsequent application

3.10
predicted Application Security Control
predicted ASC
Application Security Control in which security activities are replaced by a *PASR* (3.7)

3.11
prediction consumer
anyone that relies on an *Expected Level of Trust* (3.8)

Note 1 to entry: Mainly application consumers, application acquirers, and application owners.

3.12
prediction initiator
entity that selects an *Expected Level of Trust* (3.8) for an application

Note 1 to entry: Typically, the project team with approval by the application owner.

3.13
verification measurement
activity provided by an Application Security Control to verify if its security activity was correctly implemented and works as expected by producing required evidence/outcomes

3.14
substantial change
change that causes sufficient impact to the risk assessment so that the application owner no longer permits *predicted Application Security Controls* (3.10), resulting in the project team performing the necessary Application Security Control activities in the Actual Level of Trust

3.15
regression testing
testing required to determine that a change to a system component has not adversely affected functionality, reliability or performance and has not introduced additional defects

4 Abbreviated terms

AS	Application Security
ASC	Application Security Control
ASCs	Application Security Controls
ANF	Application Normative Framework
ONF	Organization Normative Framework

5 Prediction concepts

5.1 Goal of prediction

Predictive security occurs on a daily basis. The goal of this document is to make Application Security (AS) predictions explicit rather than implicit and to document consistently the prediction. When predictions are consistent, and correctly documented using the Expected Level of Trust Report, prediction consumers have a much better basis to make risk decisions based on the Expected Level of Trust Report. All predictions are inherently subject to uncertainty, and the accuracy of any prediction is unlikely to be any more accurate than the least accurate source.

AS predictions focus on the AS risks that exist in both original and subsequent application versions. The AS prediction is as follows: the prediction initiator believes that the subsequent application has an equivalent Level of Trust to the original application even though some of the ASC activities indicated by the Level of Trust are not completed by the project team; rather the ASC activities are replaced by a PASR. Without predictions, the only way to believe that equivalent Levels of Trust are present in the two applications is to perform all of the activities for all of the ASCs identified by the Level of Trust.

The prediction framework is one technique for gaining assurance in an application, and needs to be considered holistically with other approaches to achieving assurance, such as Regression Testing as defined in ISO/IEC/IEEE 29119-1[1] and ISO/IEC 90003[2]. This document provides assurance efficiency to the application security confidence. The efficiency comes at a cost, as there is a replacement of the activities of some of the enumerated ASCs in the Expected Level of Trust with PASRs. The application owner should be aware of this cost and should make an appropriate risk decision to accept the PASR using ONF Committee advice.

Under the application security concern perspective, the default without any guidance from the ONF Committee and approval by the application owner is that predictions are not permissible. Without predictions, the only way to have equivalent "Levels of Trust" confidence between the original and subsequent applications is for the Actual Level of Trust to be the same for both applications.

NOTE Annex B provides a comparison between an ASC and a PASR.

5.2 Prediction framework

The definition of a secure application, defined in ISO/IEC 27034-1, is when the Actual Level of Trust is equal to the Targeted Level of Trust. The prediction framework cannot and should not change the Actual Level of Trust definition. The prediction framework adds the Expected Level of Trust as a mechanism to indicate the project teams belief regarding the security properties of the subsequent application.

The prediction framework includes the following concepts:

a) An original application where the Actual Level of Trust was equal to the Targeted Level of Trust resulting in, per the ISO/IEC 27034-1 definition, a secure application.

b) A subsequent application where the Targeted Level of Trust contains a subset of the original applications Actual Level of Trust.

c) A risk analysis, documented in the PASR, as to why the subsequent application does not have a substantial change and performance of an ASC would generate the same result as during execution of the security and verification measurement activities in the original application.

d) For the subsequent application, a claim that the application has an Actual Level of Trust and a belief that the subsequent applications Expected Level of Trust is equivalent to the original applications Actual Level of Trust.

5.3 Expected Level of Trust

5.3.1 Concept

This document adds the definition of the Expected Level of Trust, which indicates that the project team does not perform the activities of specific ASCs, rather predicts that if the project team performed the ASC activities the results would match the results from the original application.

Figure 1 illustrates the basics of the Expected Level of Trust.

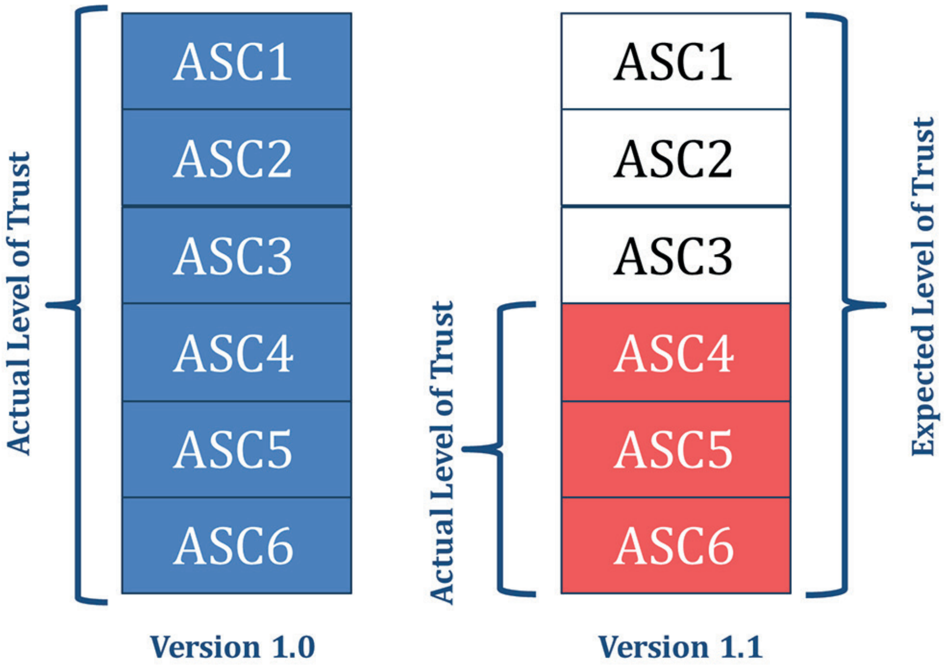

Figure 1 — Expected Level of Trust

For version 1.0, the Targeted Level of Trust was Blue and the application successfully implemented the 6 ASCs so the Actual Level of Trust was Blue. As this was the first instantiation of the application, there were no predictions and no Expected Level of Trust.

For version 1.1, the project team successfully implemented the 3 ASCs so the Actual Level of Trust is Red. The Expected Level of Trust is Blue as the project team predicts that performing the 3 ASCs activities is not necessary for version 1.1. The project team can then state that the team knows that the application is secure at the Red Level of Trust, and believes that the application is secure at the Blue Level of Trust as the remaining ASCs have an associated PASR.

An Expected Level of Trust contains an Actual Level of Trust, which is a subset of the Expected Level of Trust, and the remaining ASCs not contained in the Actual Level of Trust have an associated PASR. As a result, this complements the definition of ‘secure application’.

5.3.2 Expected level of trust in the ONF

The ONF committee establishes the guidelines for when a PASR is appropriate for each ASC in the ASC library. Figure 2 documents an ONF that contains three levels of trust and is the source of the Levels of Trust in Figure 1.

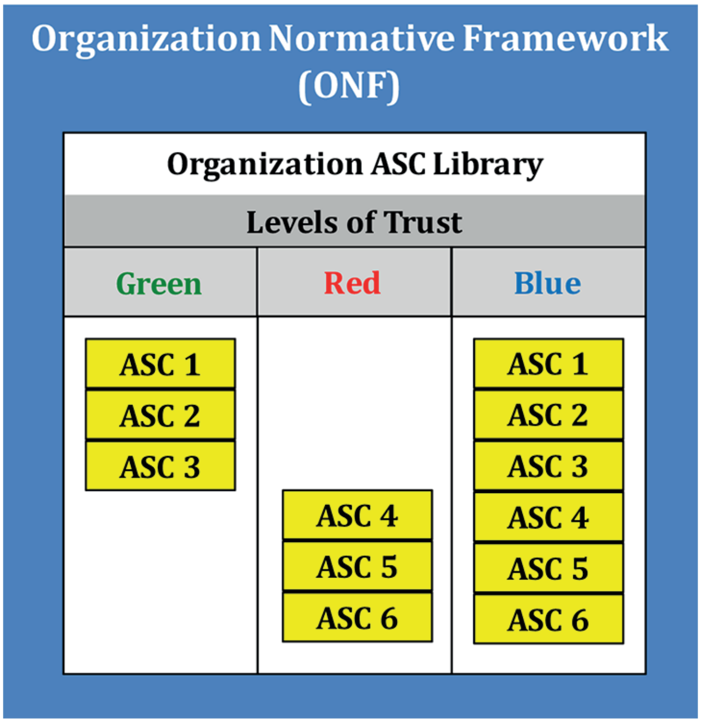

Figure 2 — ONF

The Green and Red Levels of Trust contain separate ASCs, while the Blue Level of Trust is the combination of Red and Green.

There is no special Expected Level of Trust. As Figure 1 demonstrates, for version 1.0 the Targeted and Actual Level of Trust were Blue and for version 1.1 the Expected Level of Trust is Blue. This is intentional as using the same Levels of Trust allow acquirers to compare versions of the same application with the same Level of Trust. The difference is that if the two versions have the same Actual Level of Trust the acquirer knows that the versions are equivalent due to both completing the same ASC. If the subsequent version uses an Expected Level of Trust, the acquirer knows that the prediction initiator believes the two versions are equivalent, but the evidence of that equivalence is a rationale statement.

5.3.3 Expected level of trust in the ANF

After the AS risk assessment indicates that predictions are appropriate and the application owner approves the use of predictions, the project team establishes the ANF for the application. Figure 3 shows the ANF for both version 1.0 and 1.1.

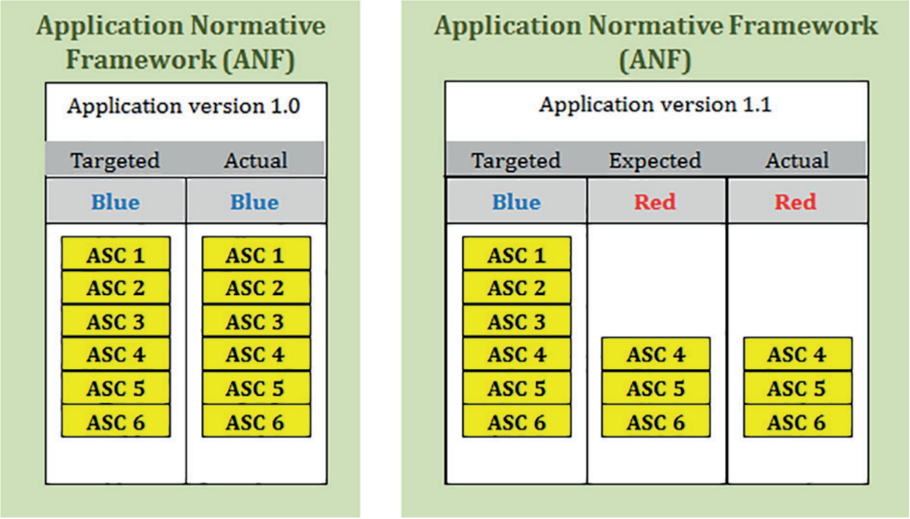

Figure 3 — ANF

For version 1.0, the Targeted and Actual in the ANF are both Blue. For version 1.1, the Targeted Level of Trust is Red, the Actual is Red, and the Expected is Blue.

All ASCs identified in an Expected Level of Trust, including those with a PASR, may be verified during an Application Security verification with an Application Security audit.

5.3.4 ASC data in the ANF

The Application Normative Framework is the repository for all data associated with an application Expected Level of Trust.

The default, without any guidance from the application owner, is that all ASC activities should occur and predications are not permissible.

For an ASC that the project team performs the activities associated with the ASC, in the ANF there is data that references the ASC and allows for the verification and auditing of the project team's execution. With a prediction, there are no activities but there is still data that references the ASC in the ANF. Figure 4 illustrates the both types of data.

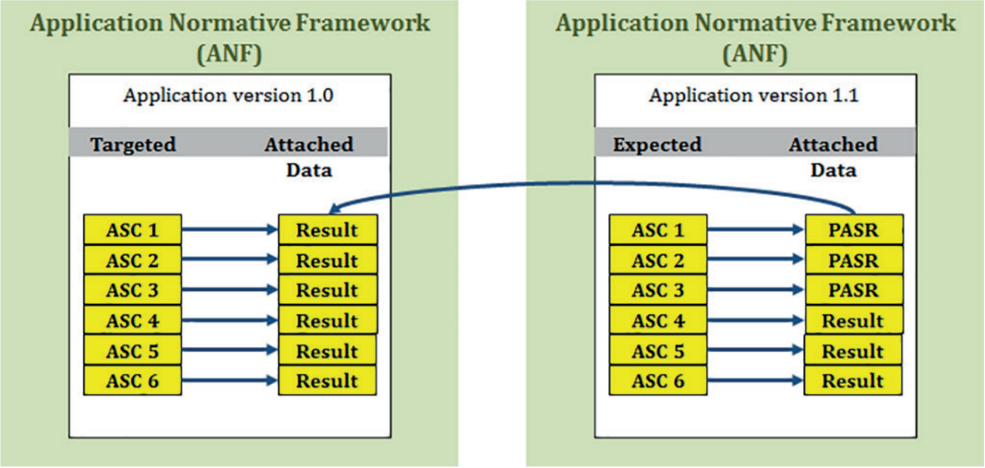

Figure 4 — ASC data

For version 1.0, each ASC has the activity data associated with the ASC stored in the ANF. For version 1.1, the project team only performs the activities for ASCs 4, 5, and 6, hence only those ASCs have associated results. For ASCs 1, 2, and 3, the project team creates a PASR. Each PASR includes the rationale as to why the activities of the ASCs are not necessary to maintain the Expected Level of Trust. The PASR also contains a reference to the Version 1.0 ANF and the results from the project team's performance of the ASCs activities.

The reference from the PASR to a prior result is mandatory. If there is no reference, there is no way for the audit team to verify the expected ASCs results when performing the audits or verifications. This reference requirement is also the underlying reason why the project team cannot use a prediction on an ASC that was never instantiated in a prior version.

NOTE Instead of a reference to the original application ANF, the ONF committee can require the project team to copy into the subsequent application ANF the ASCs result data. In that case, there is no requirement to reference the original ANF.

5.3.5 Expected level of trust over sequence of application versions

5.3.5.1 Multiple versions

The previous examples only looked at two versions of the application, but most applications have many more than two versions. The following use case follows the application versions and discusses the various Levels of Trust that the project team uses.

The project team uses the ONF from Figure 2.

The assumption for this use case is that the project team always successfully completes all activities assigned for the Target Level of Trust and, therefore, all applications are secure, as Actual equals Target.

To distinguish the various versions of the application, the application requires a unique identifier. Many schemes are available to identify and disseminate the identity. Software identifiers include ISO/IEC 19770-5[3] and ISO/IEC 19770-2[4], while hardware identifiers include ISO/IEC 20009-1[5].

5.3.5.2 Version history

Subclause 5.3.5, describes the use case, discusses the choices made by the project team and approval from the application owner, and uses Table 1 to illustrate all of the application versions.

Table 1 — Version and level history

Version	Levels of Trust	
	Actual	**Expected**
Version 1.0	**Blue**	**NA**
Version 1.1	**Red**	**Blue**
Version 1.2	**Green**	**Blue**
Version 1.3	**Green**	**Blue**
Version 2.0	**Blue**	**NA**

5.3.5.3 Original application – Version 1.0

The original application sets Targeted as Blue, completes the ASCs, and has an Actual of Blue. There is no Expected Level of Trust.

The ANF contains the results of the ASCs activities for all of the ASCs identified by the Blue Level of Trust.

The project team claims that Version 1.0 is a secure application according to the Blue Level of Trust.

5.3.5.4 Version 1.1

For version 1.1 the project team, after performing an AS risk analysis, determines that there is a substantial change in the area covered by the Red Level of Trust ASCs. The project team also determines that for the other ASCs inside of Blue, there are not substantial changes. The project team wishes to claim that the Level of Trust of version 1.1 is equivalent to that of version 1.0, so the project team sets the Expected Level of Trust to Blue.

The ANF contains the results for the Red Level of Trust ASCs and PASRs for the remaining ASCs in Blue. The PASRs contain references to the version 1.0 ANF so that the results of the predicted ASCs are linked and available.

The project team claims that version 1.1 is secure according to the Red Level of Trust and they believe it is equivalent of version 1.0 and the Blue Level of Trust.

5.3.5.5 Version 1.2

Version 1.2 is in response to a bug in version 1.1. The AS risk analysis indicates that the bug fix is only a substantial change for the ASCs that comprise the Green Level of Trust. The project team wishes to claim that the Level of Trust for version 1.2 is equivalent to version 1.1 and version 1.0 so the project team sets the Expected Level of Trust to Blue.

The ANF contains the results for the Green Level of Trust ASCs and the PASRs for the remaining ASCs in Blue. The PASRs contain references to the version 1.1 ANF, and indirectly to the version 1.0 ANF, so that the results of the predicted ASCs are linked and available.

The project team claims that version 1.2 is secure according to the Green Level of Trust and they believe it is equivalent of version 1.0 and the Blue Level of Trust.

5.3.5.6 Version 1.3

Version 1.3 is a quick response to an error in version 1.2. The AS risk analysis indicates that the bug fix is again only a substantial change for the ASCs that comprise the Green Level of Trust. The project team wishes to claim that the Level of Trust for version 1.3 is equivalent to the previous versions so the project team sets the Expected Level of Trust to Blue.

The ANF contains the results for the Green Level of Trust ASCs and the PASRs for the remaining ASCs in Blue. The PASRs contain references to the version 1.1 ANF so that the results of the predicted ASCs are linked and available. It is important to note that the PASR reference is to 1.1 and not 1.2. The reference link can be explicit or implicit by following the version 1.1 links. Either way the point is that the last time the ASCs activities were completed was in version 1.1

The project team claims that version 1.3 is secure according to the Green Level of Trust and they believe it is equivalent to version 1.0 and the Blue Level of Trust.

5.3.5.7 Version 2.0

Version 2.0 is a rewrite of the architectural infrastructure of the application. The AS risk assessment indicates that there are numerous substantial changes and no predictions are possible. Much like for Version 1.0, the project team sets the Targeted Level of Trust to Blue and does not use any predictions so there is no Expected Level of Trust.

The ANF contains the results of the ASCs activities for all of the ASCs identified by the Blue Level of Trust.

The project team claims that Version 2.0 is a secure application according to the Blue Level of Trust.

5.4 Principles

5.4.1 ISO/IEC 27034-1 principles

ISO/IEC 27034-1 defines two important principles, namely Appropriate investment for application security (ISO/IEC 27034-1:2011, 0.4.3) and Application security should be demonstrated (ISO/IEC 27034-1:2011, 0.4.4). Predictions cannot violate those principles.

5.4.2 Appropriate investment for application security principle

PASRs do not violate the investment principle because the application owner, after performing an AS risk assessment, determines that executing the ASC activities again is not necessary. Performing those activities after having determined that there is no need for the activity likely wastes resources, a direct violation of the "appropriate investment" principle.

Having the project team provide the result of the AS risk assessment, and an accompanying prediction rationale, allows the application owner or acquirer to evaluate:

a) the AS risk assessment;

b) the assignment of the Expected Level of Trust;

c) the list of ASCs that have a PASR; and

d) the appropriateness of the Expected Level of Trust for the intended use of the application.

5.4.3 Application security should be demonstrated principle

PASR do not violate the demonstration principle, as there is evidence of the action taken. When the project team performs an ASC, the result is a verification measurement that the auditor reviews in step 5 of the ASMP (ISO/IEC 27034-1:2011, 7.3.6). The audit process reviews the verification measurement and determines that the expected result is present.

When dealing with a prediction, the auditor performs the same type of operation; namely, the auditor:

a) reviews the PASR and determines that the use of the PASR meets the guidelines established by the ONF committee;

b) audits the PASR to verify that:

    1) the PASR references the ASC from the original application;

    2) the expected outcomes of the original application ASCs, as produced during the original application implementation actually exist; and

    3) the PASR includes a prediction rationale statement, as explained in 9.3.2.

5.5 Prediction authorization

5.5.1 Prediction accountability

Predictions require two authorizations, the first from the ONF committee, and the second from the application owner.

a) The ONF committee should establish the ground rules for each ASC in the organization ASC library clarifying under what circumstances prediction is permissible. The ONF committee reviews, on an ongoing basis along with all other ASCs activities and outputs, the AS prediction guidelines. During the review, the ONF committee ensures that the guidelines still reflect appropriate risk guidance.

Without ONF guidance on prediction ground rules, the default is that predictions relative to the ASC are not allowable.

b) The application owner, using the AS prediction guidelines established by the ONF committee and after appropriate AS risk assessment, determines that an Expected Level of Trust is appropriate.

For each ASC that the project team generates a PASR for instead of performing the ASC activities, the project team reviews the AS risk assessment to verify that the PASR is appropriate for the indicated risk.

5.5.2 Forced authorization

Neither ONF committee nor application owner can force the other to accept the use of predictions.

The ONF committee cannot force the application owner to skip execution of the ASC activities. The application owner sets a Target Level of Trust that includes the ASC, perform the activities, and accomplish an Actual Level of Trust. There is no prediction as the project team performed the required activities.

The application owner cannot force the ONF committee to accept predictions outside of the established guidelines. Certainly, the application owner can request updated guidelines, but if the guidelines do not change, and the project team does not perform the ASC activities, the ONF committee does not allow the use of the desired Expected Level of Trust.

5.6 Claims relative to the actual level of trust

The project team, when delivering the original application to acquirers, may make security related claims relative to the original application. One goal of predictions is to help the project team relate the claims of the original application to the subsequent application even though the subsequent application has a different Actual Level of Trust.

The original application may have additional security claims based on additional mechanisms. If the original application does undergo additional mechanisms, the project team can attempt to show the transfer of the additional mechanism to the subsequent application based on the Expected Level of Trust. The efficacy of this transfer is outside the scope of this document; and it is mechanism-specific.

Mechanisms that can generate the additional security claims include, but are not limited to:

a) ISO/IEC 15408 (all parts)[3];

b) ISO/IEC 15026 (all parts)[4].

6 Predictions

6.1 Prediction initiator

The initiator of the prediction is typically the project team under direction of the application owner. The team, when presenting the risk assessment to the application owner (ISO/IEC 27034-1:2011, 7.3.3), indicates that the subsequent application does not need to perform certain ASCs. After review of the guidelines established for predicating the ASC, established by the ONF committee, the application owner approves the Actual Level of Trust, which does not contain the predicted ASCs, and the use of the Expected Level of Trust that does contain the predicted ASCs.

6.2 Prediction circumstances

6.2.1 Typical circumstance

The circumstance aspect is a reason why there is a subsequent application. The circumstance aspect is a major factor in the risk assessment. Circumstances for subsequent applications are varied but include and are not limited to:

a) New functionality. Adding new functionality, depending on application architecture, can lead to large sections of the application that do not need verification. If there is no repeat of verification, then predictions may be an alternative.

b) Bug fixes:

   1) Fixing bugs normally focuses on changes with many functions of the application not needing re-verification. If there is no repeat of verification, then predictions may be an alternative. Expanding the targeted contexts

   2) The functionality of the application remains the same but now the types of threats and supported environments expand. This type of change to the application can represent a minor change or a massive rewrite of substantial portions of the application.

6.2.2 Relationship to level of trust

The assumption, made by both the prediction initiator and the prediction consumer, is that the Level of Trust is consistent between versions of the application. While normally true, there are circumstances where there is a desire to change the Level of Trust between versions. The following examples provide suggestions as to how the project team responds to changing Levels of Trust.

a) Version 1.0 Level of Trust is insufficient to mitigate the identified threats.

   The project team's first response is going to be to select a new Level of Trust that has additional ASCs that mitigate the identified threats. For each new ASC, there is no possibility of prediction, as there are no previous results to reference in the PASR. Hence, the project team executes on all new ASCs.

   It is likely that the new Level of Trust contains ASCs that are in the previous Level of Trust. The project teams, following the AS risk assessment, can determine that predictions are appropriate for ASCs executed in the original application. The resulting ASCs would have a PASR referencing the activities in the original applications ANF.

   This situation is analogous to finding a vulnerability in the original application; the response is to change the ASCs to mitigate the vulnerability. The application has never executed the new ASCs. Hence, predictions are not possible and for the subsequent application the project team executes the new ASCs activities.

6.3 Prediction consumer

While the prediction initiator can make any claim they wish regarding the transfer of security claims, the prediction consumer is the final arbitrator of the prediction. If the prediction consumer accepts the Expected Level of Trust Report, then the prediction consumer is accepting the risk assessment regarding the changes and agreeing with the project team that the changes in the subsequent application are not substantial.

The prediction initiator cannot force the prediction consumer to accept the Expected Level of Trust Report. The prediction consumer, through their own risk decision using the supplied rationales, may only accept the Actual Level of Trust. This certainly implies that any predictive claims made relative to the original application do not transfer to the subsequent application according to the prediction consumer.

To accept an Expected Level of Trust Report, some prediction consumers can require additional evidence, different rationale bases, or a myriad of other types of review. These additional prediction consumer requirements are very likely unanticipated when the application owner approves the use of predictions. It is therefore common that prediction consumers miss what is, for them, a critical data point that affects their risk decision of the Expected Level of Trust Report. While there can be a desire by the project team to provide the missing data, it can be impossible to generate the extra data long after the application has completed its development. Prediction consumers who have special data requirements should therefore make those requirements visible to their application providers in a manner that prediction initiators are better prepared to generate the data necessary for these prediction consumers to have a sufficient level of confidence in the Expected Level of Trust.

7 Substantial changes

7.1 Definition discussion

As stated in 3.14, the definition in use for substantial is, "change that results in sufficient impact to the risk assessment so that the application owner no longer accepts the risk of a prediction resulting in the project team performing the ASC activities". The focus on the risk assessment is critical. Other definitions are industry, vendor, application, culturally, and geographically different. What is substantial for one is not substantial for another. The definition puts the onus on the application owner to assess the risk and determine the result based on the current circumstances for the subsequent application.

If each version of an application was independent from all previous versions of the application, there would be no need for predictions. That is not the case; version 1.1 is intimately bound to version 1.0. More importantly, those using the various versions of the application expect a consistent, within a small range, set of properties for the application. The application owner may set a different Targeted Level of Trust for the different versions. In the absence of any specific comment from the project team, the expectation from the acquirer is that version 1.1 is equivalent to version 1.0.

7.2 Guidance for substantial changes risk analysis

7.2.1 General

As the determination of a substantial change is the result of a risk assessment, there is no simple explanation of what is and is not substantial change. The application owner should determine at the time what changes are substantial and which are not. This guidance attempts to illustrate what can be appropriate or not to determine substantial when performing the risk assessment.

One aspect of substantial change determination is the type of activity the ASC requires. Some activities are critical no matter what change occurs; others can be situation-dependent. The following examples are examples only and each application owner needs to make their own appropriate determinations.

7.2.2 Code change and static analysis

In this example, the ASC in question requires static analysis of all modified code. The ONF committee attaches to the static analysis ASC that predictions are not permissible. Any code change requires static analysis.

If the application owner decides to allow a prediction and not perform static analysis, the Application Security Rationale needs to provide compelling reasons to skip this ASC activity. It is likely that, even with compelling rationale, prediction consumers of the application rejects the rationale. This highlights the fact that, while the application owner and project team believe they have a valid reason to skip ASCs activities, the prediction consumer makes the final risk decision if the Expected Level of Trust is acceptable.

7.2.3 Architectural review

In this example, the ASC activity is a security architecture review. The ONF committee indicates that predictions are appropriate when the project team justifies that changes do not affect the architecture. The guidelines include examples such that changing data buffer sizes does not normally change the security architecture.

After appropriate review, the application owner determines that no changes to the security architecture are occurring and the Target Level of Trust does not contain the security architecture review ASC. The project team generates the Application Security Rationale and, during the audit, the audit team verifies the existence of the Application Security Rationale. Assuming that all ASCs are complete, the Actual Level of Trust matches the Target Level of Trust, and the Expected Level of Trust contains the security architecture review ASC. This security architecture review ASC is a predicted ASC.

7.2.4 Deprecation of tests over time

When assessing the risk of a substantial change, the risk assessment would include an analysis of the test suites in use to generate the ASC activity evidence. The techniques in use to generate the ASC evidence change over time. The techniques adjust to improvements in methods and knowledge gained from previous testing. The result is that, due to changes in techniques, an ASC that previously passed can now fail.

The project team, in their substantial risk analysis, needs to include the possibility of changes to the testing techniques, especially when the project team uses a PASR for several generations of the application. To assist the project teams, and the application owner, the ONF committee can set maximum limits on the use of consecutive PASR for a specific ASC.

8 Confidence

8.1 Confidence building blocks

Confidence by itself is meaningless. The real term is confidence in something by someone. In this document, the “something” is the confidence in the risk analysis performed by the project team that a change is not substantial. The “someone” is the prediction consumer. The prediction consumer needs to have confidence in the project team, and their risk analysis, to believe that the properties of the original application are still present in the subsequent application.

Confidence in the transfer of properties from the original to subsequent application has no relationship to the functionality of either application. Trust in the functionality comes from other mechanisms and this document makes no statement relative to this trust.

8.2 Establishing confidence

Confidence in the Expected Level of Trust increases through two main mechanisms: evidence and history. For predictions, the evidence is the Application Security Rationale and the history is sequence of versions along with the claims and experience associated with the sequence.

Confidence is an attribute of the prediction consumer, their experience with the application sequence raises or lowers their confidence in a specific Expected Level of Trust for a specific application. An application sequence that requires constant updating due to build issues lowers the prediction consumers’ confidence that a specific Expected Level of Trust is present.

The evidence available is that arising directly from the prediction framework activities, as well as indirectly from other activities such as Regression Testing, which application teams often perform to verify or validate that the capabilities of the software have not been compromised by any change(s).

9 Prediction application security rationale

9.1 Linkage to ASC

A Prediction Application Security Rationale (PASR) is directly bound to an ASC belonging to the ANF. The binding can be direct, in that, the repository for the ASCs also contains the PASR, or the binding can be through links that indicate the storage location of the PASR.

9.2 Components

Without regard to how the project team binds the PASR to the ASC, the following information is present in the PASR:

a) Identifiers:

    1) Identifier of ASC associated with this prediction;

    2) Identifier of original application;

    3) Identifier of subsequent application;

    4) Identifiers in this context can be text strings, GUID, or other structured identifiers.

b) Actors:

    1) Prediction initiator – Typically this is the project team, but other entities also can initiate a prediction.

       It is possible that other entities can request a prediction but only the project team is capable of substituting ASC activities with a PASR.

    2) Application owner – Role of the person accountable for the Application Security (AS) of this project.

       Approves the proposed prediction for a specific ASC.

    3) Prediction consumer – Roles of the prediction consumer would include buyers of the application, other business units inside the same organization including the application as a component, or users of products that included the application as a component.

       The prediction consumer reviews the prediction rationale when making a risk decision to determine if an application update is appropriate to use.

c) Prediction circumstances

    1) The underlying reasons for creating the subsequent application.

    2) Under what circumstances predictions are likely to be true.

    3) Under what circumstances predictions are likely to be false.

d) Rationale

    1) Risk analysis for the identified ASCs as to why the activities specified in the ASC are not necessary for the subsequent application

    2) Prediction confidence

       i) How confident the prediction initiator is that the prediction is correct;

       ii) The project team can improve confidence in the prediction by obtaining additional evidence relative to the prediction. Such evidence can come from partial verifications based on techniques such as regression testing and retesting. See ISO/IEC/IEEE 29119-1[1] for details on testing techniques.

3) Statement that change in the subsequent application is not substantial and there is no need to execute the ASCs activities.

e) ASC outcome from original application

1) Verification measurement values or the PASR associated with the ASC.

2) If the ASC is not present in the original application then a prediction is not permissible.

f) Supporting criteria for the prediction. The Application Security Rationale, which includes the rationale from the application owner as to why the risk analysis supports the exclusion of the ASC activities for the application.

9.3 Format

9.3.1 Identifiers, actors, ASCs outcomes

The format to describe the identifiers, actors, and previous ASCs outcomes are ONF specific. The ONF committee determines what is sufficient in their organization and establish the necessary formats.

9.3.2 Rationale

The rationale is a statement, in free-flowing text, which describes the analysis, circumstances, and confidence. It is likely that the analysis repeats for multiple ASCs in the ANF. This is not surprising, as the circumstances do not change for an individual ASC inside of the ANF. The goal of the individual ASC rationale statements is to combine into an Expected Level of Trust Report. There is no requirement for the individual ASC rationale statement to repeat fixed information. Rather, the rationale can point to a central location where the text is available.

9.3.3 Duplication of information

An individual PASR provides information to help fill out the Expected Level of Trust Report. The identifiers, actors, and prediction circumstances are the same for every PASR in the Expected Level of Trust Report. The expectation is that an individual PASR points to the shared information in the Expected Level of Trust Report and not duplicate the information in the PASR.

9.3.4 Assurance cases

As the Expected Level of Trust Report contains claims made by the application team, a format that helps quantify claims is desirable. Annex A details one example of the use of assurance cases from ISO/IEC 15026-2[7].

9.4 Approval by ONF Committee

The ONF Committee establishes the guidance for predictions and the use of the PASR for each ASC. The committee has three choices:

a) No predictions

1) The committee determines that the activities for the ASC are critical for all applications. No ANF can specify that the completion of this ASC uses a prediction.

   2) Examples of this type of blanket refusal can include static analysis for all changed code or code backup.

b) Predictions with conditions

   1) The conditions that the committee approves are going to be specific to the ONF. The conditions can specify both positive, as in you can predict given X, and negative, as in you cannot predict if Y.

      The determination of the existence of the conditions is a function of the ANF.

   2) Examples of these conditions can include:

      i) after 5 application versions with a prediction, the team should perform the ASC;

      ii) incident response teams can always predict this ASC; and

      iii) if this function changes, you cannot predict.

c) No restrictions

   The ONF committee determines that there is no need to restrict predictions for the ASC and the ANF can always specify a prediction for the ASC.

9.5 Use of RACI charts in description of activities, roles, and responsibilities

This document uses RACI charts for assigning roles and responsibilities for carrying out activities in processes. Such charts identify actors responsible, accountable, consulted, or informed for the realization of an activity. Table 2 enumerates the abbreviations in use to describe the actor's role.

Table 2 — Abbreviations for responsibilities used in RACI charts

Code	Responsibility
R	Responsible for the realization of an activity
A	Accountable for the realization of an activity
C	Consulted during the realization of an activity
I	Informed of the realization of an activity

10 PASR audit

10.1 Auditing linkage

Auditing is the subject of ISO/IEC 27034-1:2011, 7.3.6. The goal at this step is to ensure that the Targeted Level of Trust matches the Actual Level of Trust. The auditor reviews the verification measurements provided by the ASCs and verifies the attainment of the expected results.

10.2 Auditing actual level of trust

There is no change to the auditors' actions for ASCs that represent the Actual Level of Trust. The auditor reviews the verification measurement data and if it meets the specified requirements, the project team has met the Actual Level of Trust.

10.3 Auditing expected level of trust

The auditor verifies that for the predicted ASCs, the project team provides the PASR. If the PASR is present, the auditor can indicate that the project team has met the Expected Level of Trust.

From an auditor standpoint, the actions of the auditor are the same when auditing for verification measurement data or PASR. The auditor validates that the data is present and that it conforms to the ONF guidelines.

10.4 PASR quality

The auditor does not examine the quality of the PASR, which occurs in validation. The auditor does confirm that the form and function of the PASR are present and meet the guidelines as specified by the ONF Committee.

11 PASR Verification

11.1 Validation

The audit team should validate PASRs in the Expected Level of Trust by examining the quality of each of its components (as enumerated in 9.2), and their conformance to ONF Committee directives (see 9.4). The audit team should consult the ONF Committee for the required expertise in technical matters.

11.2 Verification

Verification is a base principle of ISO/IEC 27034-1. The audit team, when performing step 5 (ISO/IEC 27034-1:2011, 7.3.6) may rerun some of the actions required by the ASC. The audit team may select any number of ASCs to rerun, from all to a sample set (e.g. statistical, risk based, etc.). There is no change when dealing with predictions and PASR in particular. The audit team can pick a sample set and then run the activities specified by the ASC.

The use of an Expected Level of Trust does not place any requirement on the audit team to use a different mechanism when establishing the statistical sample of ASCs to audit. When the audit team does use a different mechanism to sample differently between the Actual Level of Trust and the Expected Level of Trust, the audit team should document the differences between the two selection mechanisms.

11.3 Expected results

The prediction is that there is no need to perform the ASC activities as the change in the subsequent application is not substantial and, hence, the activities do not add to the expected security properties of the application. If the audit team picks an ASC for demonstration that the activities are correct, the audit team runs the activities just as the ASC requires and the expected result is that the team can generate the correct verification measurements just as if the project team did perform the ASC.

11.4 Missing state

11.4.1 Inability to generate verification measurements

It is possible that the ability to rerun ASC activities is not present. While rare, it is possible that the circumstances and infrastructure necessary to perform the ASC activities are no longer available. If this condition occurs, the audit team either accepts the PASR or finds another way to generate verification measurements.

11.4.2 Example

For example, the ASC in question requires a simulation of a specific set of operations and the verification measurement is the output from the simulation. The simulation ran a year or so prior to the availability of hardware and takes over 3 weeks to run. The project team did not run the simulation. There is a

PASR for why the simulation did not execute. The audit team has the prediction but is unable to run the simulation because:

a) the simulation environment no longer supports the subsequent application. Operations or test cases are not current with the simulation environment.

b) the time necessary to run simulation environment is not available.

   1) The current simulator is fully engaged with another project.

   2) The audit and project team cannot wait three weeks for the verification measurements.

The audit team has a choice in this circumstance; accept the PASR or look for other ways to gain the verification measurements. Accepting the PASR can be viable, but consider again the nature of the example; the tests run on a simulation. On projects that do simulations, normally a connected activity runs the same tests on the resulting hardware. The audit team can skip the simulation and run the related tests on the real hardware. While not exactly performing the tests in simulation, the demonstration that the subsequent application would pass the audit verification is possible.

12 PASR implementation

12.1 Prediction framework

The steps, identified in 12.2, represent the prediction framework. The framework, at its essence, is to create an Expected Level of Trust that matches a previous Actual Level of Trust of the application and then create PASRs for one or more ASC not performed.

12.2 Steps to implement a PASR

12.2.1 General

a) ONF Committee establishes guidelines.

   1) The ONF Committee, for each ASC in the organization ASC library, determines the circumstances when predictions are appropriate and inappropriate. The ONF Committee stores these guidelines as part of the ASC in the ASC library.

   2) Table 3 defines the RACI responsibilities for PASR implementation.

b) Project team performs the risk analysis of the subsequent application (in accordance with ISO/IEC 27034-1 ASMP –step 2), and updates the application's Targeted Level of Trust" as needed.

c) Project team selects ASCs for ANF. The selection of the ASCs follows the process defined in ISO/IEC 27034-1.

d) Project team performs further risk analysis to determine substantial changes.

e) Project team refines the Target Level of Trust based on substantial changes and creates the Expected Level of Trust.

f) Application owner approves the prediction and the use of PASR and the Expected Level of Trust.

g) Project team develops the subsequent application associated with ANF and performs activities related to each ASC in the ANF, including the performance of verification measurements or generation of ASR.

h) Application audit team verifies existence of verification measurement or PASR for each ASC in the ANF.

i) If all ASCs verification measurements were successfully performed and all PASR were approved, then the subsequent applications Expected Level of Trust is achieved.

j) Project team generates the Expected Level of Trust Report.

12.2.2 Actor responsibilities

Table 3 presents a RACI chart for process “Implement a PASR".

Table 3 — Responsibilities during PASR implementation

Realization activities	ONF committee	Application owner	Project team	Verification team	Audit team
a) Establish guidelines	A/R	I	I		I
b) Risk analysis		A	R	I	I
c) Select ANF	I	A	R	C	I
d) Substantial change		A	R	C	I
e) Create Expected Level of Trust	I	A	R	C	I
f) Approve Expected Level of Trust	I	A	R	C	I
g) Develop application		A	R	I	I
h) Verify ASCs		A	C	R	I
i) Verify Actual Level of Trust and Expected Level of Trust		A	C	C	R
j) Generate Expected Level of Trust Report	I	A	R	C	C

12.3 ONF feedback

The project team can encounter challenges with the ASC definition, especially with the guidelines as to when it is permissible to use a prediction. As with all ASCs definition issues, the project team corresponds with the ONF Committee attempting to clarify or change the ASC (ISO/IEC 27034-1:2011, 8.1.3.2 f). This process is the same for PASR. As the PASR guidelines are part of the ASC, feedback to the ONF Committee uses the same mechanism.

It is likely that project teams wish for a quick response from the ONF Committee, especially when the project team is responding to an application vulnerability. In these cases, the ANF to ONF feedback mechanism should have provisions for extremely quick issue resolution.

13 Expected level of trust report

13.1 Purpose

The main purpose of Expected Level of Trust Report is to allow acquirers of the subsequent application the ability to make risk decisions based on the risk analysis from the project team. The content of the report provides sufficient data that the project team’s risk analysis is reasonably accurate. Perfection is not possible due to the inherent variability due to predictions.

13.2 Components

The Expected Level of Trust Report should contain the following:

a) Identifiers

   1) Original application identifier;

   2) Subsequent application identifier;

   3) Application identifiers need to be unique such that there is no ambiguity as to which version of the application the Expected Level of Trust Report is referencing. Application versioning is a form of asset management and ISO/IEC 19770-5[3] provides guidance on IT asset management.

b) Actors

   1) Prediction initiator – Typically this is the project team, but other entities also can initiate a prediction;

   2) Application owner – Identifies the entity approving the prediction.

c) Prediction circumstances. The underlying reasons for creating the subsequent application.

d) Levels of Trust

   1) Actual Level of Trust for original application;

   2) Expected Level of Trust for original application (if used);

   3) Actual Level of Trust for subsequent application;

   4) Expected Level of Trust for subsequent application.

e) Predicted ASCs

   1) List of ASCs that are predicted: While possible to recreate the list by comparing the Expected Level of Trust with the Actual Level of Trust, this list makes it explicit and hopefully easier for prediction consumers;

   2) For each predicted ASC, the Prediction Application Security Rationale.

f) Rationale. The circumstances and the set of predicted ASCs as to why these items meet the Expected Level of Trust.

13.3 Format

The report is free form text. The prediction consumer is going to read and make risk decisions based on the information. There is no requirement for machine-readable formatting of the Expected Level of Trust Report.

13.4 History, assumptions and social history

The components in the report tell much of the story between the original and subsequent applications. When a prediction consumer makes a risk decision, additional information can be critical to that decision. It is difficult to determine what additional information is necessary. The following items are examples only and individual prediction consumers have their specific requirements.

a) History

   1) It is likely that the original and subsequent applications are not version 1 and version 1.1, there is a much larger history of versions. The trust and experience of each version factor into the prediction consumers' risk decision.

   2) The Expected Level of Trust Report therefore may contain information relative to all of the previous versions of the application.

b) Assumptions

   1) The prediction initiator makes assumptions regarding the subsequent application in relation to contexts, use frameworks, supply chains, and many other factors. Use of the application outside of these assumptions may affect the prediction consumers' risk decision.

2) The Expected Level of Trust Report therefore may contain information relative to the assumptions the prediction initiator makes relative to the application.

c) Social history

1) There can be a large body of comments relative to the application from sources not related to the application developer. These comments can be both positive and negative and can be unbiased or not. Prediction consumers can use these statements in making their risk decision.

2) Attaching links or excerpts from reviews relative to versions of the application can assist the prediction consumer. It is the responsibility of the prediction consumer to determine the validity, and degree of bias, when using social history information relative to the subsequent applications in their risk decision.

Annex A
(informative)

Expected level of trust assurance case

A.1 Format recommendation

As the Expected Level of Trust Report is making the claim that the Expected Level of Trust for the subsequent application has a relationship to the Actual and/or Expected Level of Trust in the original application, the recommendation is to use of ISO/IEC 15026-3[7] to document the claim.

A.2 Prediction claim

A.2.1 Context

The prediction initiator claim is that the subsequent application has nearly the same security properties as the original application.

The subsequent application is a subsequent version of the original application (i.e. original is version 1.0 and subsequent is version 1.1). The claim is that security properties of the original are present in the subsequent application.

A.2.2 Related consequences

The consequence of the relationship between the original and subsequent applications is that acquirers can make appropriate risk assessments based on the Levels of Trust.

A.2.3 Property and limitations on its values

The basis for a prediction is that the original application, at some point in the version chain, performed the activities of the associated ASCs. If no previous version of the application performed the ASC activities, then no prediction is possible.

A.2.4 Conditions and limitations on applicability

The project team, when performing their risk assessment of the subsequent application, creates a definition of substantial. That definition, when approved by the application owner, allows for the prediction of ASCs where the change is not substantial.

The claim should indicate, through appropriate rationale, that the changes are not substantial and the predictions are appropriate.

A.2.5 Duration

When the original application performs the ASC activities and the subsequent application generates a prediction, there is no issue with duration. Duration concerns begin when the original application used a prediction and the subsequent application uses a prediction. How deep can the prediction change go? The answer comes from the ONF Committee and is part of the guidelines established for predictions by the ONF.

A.2.6 Uncertainty limitations

While the same controls are in use for both applications, subtle changes in architecture, design, or implementation, can result in new and unanticipated vulnerabilities. The same is true however, for original application, there is no guarantee that following the process for the original application did not result in unanticipated vulnerabilities. The process provides an assurance, not a guarantee, that the vendor followed the defined development process and that the process discovers vulnerabilities. One example of this type of assurance, without guarantee, is the flaw remediation process inside of Common Criteria.

A.2.7 Argument

There is a degree of confidence that the Expected Level of Trust for the subsequent application matches the Actual or Expected Level of Trust for the original application because of the controls and risk analysis applied by the project team.

The subsequent application achieved a verified Actual Level of Trust using the same controls in use for the original application. The predictions that the ASC listed in the Expected Level of Trust are also present provided the basis for claiming the matching of original to subsequent applications.

A.2.8 Justification

The organizational controls that created the original application, when used to create subsequent application, result in the same security claims for the subsequent application that were available for the original application. By substantially maintaining the same process, architecture, design, and implementation, the vendor can extend the security claims in the original application to the subsequent application.

A.2.9 Evidence

The evidence includes the items listed in 13.2

A.2.10 Objective criteria

Risk analysis that shows the changes are not substantial.

Annex B
(informative)

Comparison of ASC to PASR

Annex B provides a comparison between an ASC and a PASR. While the ASC fully contains the application security rationale, there are some differences and Table B.1 highlights the similarities and differences.

Table B.1 — Comparison of ASC to PASR

	Application Security Control (ASC)	**Predictive Application Security Rationale (PASR)**
Definition	An ASC is a set of security activity and verification measurement activity used to mitigate an AS risk to an approved acceptable level, and be able to demonstrate it.	A PASR is a rationale used to justify why an application project team decided not to perform again the verification measurement of a specific ASC. NOTE A PASR can only be used for an ASC for which the security activity was already performed.
Purpose	a) Address an application security requirement. b) Ensure that unacceptable application security risks are adequately mitigated. c) Provide verifiable evidence to support claim that an application is secure.	a) Lower cost of implementing and verifying security in applications. b) Speed up implementation of security in an application. c) Provide rationale to support claim that a subsequent version of an application is expected to be secure.
Development process	**Process for building an ASC** (described in ISO/IEC 27034-2) This process is part of the ONF Management Process. a) Define a rationale to address an application security requirement. 1) Rationale supporting that activities included in this ASC are implementable, produces clear outcomes to address the requirement and really mitigate the related risks. 2) Rationale supporting that outcomes produced by the security activities are verifiable, when and how they should be measured, verified and compared with expected outcomes. b) Get this rationale approved.	**Process for writing a PASR** (described in this document) a) Define a rationale to justify why an ASC does not need to be implemented or verified, and is replaced by this PASR. Rationale supporting why a specific ASC does not need to be implemented and verified, accordingly to the three principles presented in this document. b) Get this rationale approved as an acceptable way to bypass the ASC implementation/verification and maintain a “predictive level of trust” that is equivalent to the targeted level of trust because the organization considers that: — implementing this PASR has no impact on the AS requirement; and — the AS risk is still mitigated on the acceptable level.

Table B.1 *(continued)*

	Application Security Control (ASC)	**Predictive Application Security Rationale (PASR)**
	c) Assign this ASC to one or many Levels of Trust in the Organization's ASC Library, identify its owner, and dates such as when this ASC needs to be distributed for training, implementation, and expiration. NOTE The knowledge and criteria, including expected results, supporting the claim than an ASC correctly addresses specific AS requirements (why) and adequately mitigates related AS risks to an acceptable level, are directly embedded in this ASC section by domain experts who develop, validate and verify this rationale/strategy before the development of an ASC.	NOTE The knowledge and criteria supporting the claim than a PASR can replace an ASC, are directly embedded in this PASR section by domain experts who develop, validate and verify this rationale during the development of a PASR.
Security activity to mitigate risks	a) Define the application security process/component implemented in this ASC, specifying: 1) what activities are performed; 2) how these activities are performed (e.g. best practices, libraries, tools, parameters, etc.) including expected outcomes; 3) where these activities are performed (e.g. in a process, on an actor, inside a component, by developing a new component like a watchdog, etc.); 4) who performs these activities (e.g. actor, responsibilities and required qualifications, if needed, for each activity); 5) when these activities are performed (before, during or after a specific activity area existing in the ASLCRM); 6) how much it costs to perform these activities. NOTE 1 The knowledge and criteria to correctly implement a Security Activity is directly embedded in this ASC section by domain experts who develop, validate and verify it before the deployment of an ASC. NOTE 2 The security activity of an ASC can be seen as an application security implementation design pattern to address specific AS requirements, and to adequate mitigate AS risks to the expected/approved acceptable level.	None. NOTE 1 The original ASC replaced by this PASR does not need to be re-implemented or re-verified. NOTE 2 The impact is the application AS risks, addressed by the ASC replaced by the PASR, possibly not mitigated to the expected level.

Table B.1 *(continued)*

	Application Security Control (ASC)	**Predictive Application Security Rationale (PASR)**
Verification measurement activity for risk mitigation	a) Define a verification measurement process for verifying that a security activity was correctly implemented, specifying: 1) what activities are performed; 2) how these activities are performed including expected outcomes; 3) where these activities are performed; 4) who performs these activities (e.g. actor, responsibilities and required qualifications, if needed, for each activity); 5) when these activities are performed (before, during or after a specific activity area existing in the ASLCRM); 6) how much it costs to perform these activities. b) Validate ASC defined and test/verify its implementation and verification and its assigned level of trust. c) Get the final approval from the ONF committee to integrate this ASC in the ASC Library for training and implementation. NOTE 1 The knowledge and criteria to correctly verify a Security Activity is directly embedded in this ASC section by domain experts who develop, validate and verify this Measurement Verification Activity before the deployment of an ASC. NOTE 2 The Measurement Verification Activity of an ASC can be seen as an application security verification design pattern for a specific ASC.	None. NOTE 1 The original measurement verification activity replaced by this PASR does not need to be performed. NOTE 2 The impact is the application AS risks, addressed by the ASC replaced by the PASR, possibly not mitigated to the expected level.
Verification process	**Process for implementing and verifying an ASC** (described in ISO/IEC 27034-3) Implementing and verifying an ASC is performed during the ANF Management Process. a) The security activity described in the ASC is implemented according to its description (what, how, where, who, when). b) The verification measurement activity described in the ASC is implemented according to its description (what, how, where, who, when), taking in account criteria and outcomes produced by the security activity.	**Process for implementing a PASR** (described in this document) Implementing a PASR means writing it according to the PASR rules and guidelines put in place by the ONF Committee. a) An ad hoc rationale is written, to support the claim that an ASC's activities do not need to be performed again for the current version of the application. b) This claim (PASR) is presented to the auditor, or the application owner to justify a missing ASC.

Table B.1 *(continued)*

	Application Security Control (ASC)	**Predictive Application Security Rationale (PASR)**
Audit process	**Process for auditing ASCs** (described in ISO/IEC 27034-4) This process can be performed anytime during the ASMP. a) Application security audit criteria and parameters are defined. b) An audit is performed, on request, accordingly to the accepted criteria. 1) The auditor verifies if compliant outcomes produced by ASC implementation/verification exist for the audited application. 2) The auditor reruns some ASC's verification measurements (e.g. 10 %, randomly selected) and compares the outcomes with those recorded by the organization, to detect any outcomes forgery.	**Process for auditing PASRs** (described in this document) This process can be performed anytime during the ASMP. a) AS Audit criteria are defined/presented. b) An audit is performed, on request, accordingly to the accepted criteria. 1) The auditor verifies if compliant outcomes produced by ASC implementation/verification exist for the audited application. 2) The auditor verifies PASRs presented in lieu of outcomes produced by ASC implementation/verification, according to the PASR rules and guidelines put in place by the ONF committee. 3) The auditor reruns some ASC's verification measurements (e.g. 10 %, randomly selected) and compares the outcomes with those recorded by the organization, to detect any outcomes forgery.

Bibliography

[1] ISO/IEC/IEEE 29119-1, *Software and systems engineering — Software testing — Part 1: Concepts and definitions*

[2] ISO/IEC 90003, *Software engineering — Guidelines for the application of ISO 9001:2008 to computer software*

[3] ISO/IEC 19770-5, *Information technology — IT asset management — Part 5: Overview and vocabulary*

[4] ISO/IEC 19770-2, *Information technology — Software asset management — Part 2: Software identification tag*

[5] ISO/IEC 20009-1, *Information technology — Security techniques — Anonymous entity authentication — Part 1: General*

[6] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

[7] ISO/IEC 15026 (all parts), *System and software engineering — Systems and software assurance*

[8] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ICS 35.030

Price based on 29 pages