

SYNOPSIS

93
103

Number and Title of the Indian Standard: IS/ISO/IEC 27034-7:2018
Information technology — Application security —Part 7: Assurance prediction framework

a) 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

b) Salient features of content:

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:

- 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;
- providing the results of a risk analysis that contains the rationale as to why the changes in the subsequent application are not substantial;
- applying to application projects that are using an Application Normative Framework (ANF);
- indicating the Actual Level of Trust for the original and subsequent applications;
- indicating the Expected Level of Trust for the original, if used, and subsequent applications;
- 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
- verifying a PASR when the auditor chooses to rerun the corresponding ASC verification activity.

c) Types/grades/classes, if any covered in the standard: No

d) Disclaimer (to be automatically provided by the program/software)