

ISO/IEC 27034-7:2018 (E)

Information technology — Application security — Part 7: Assurance prediction framework

Contents

| | |
|---------|---|
| | Foreword |
| | 0 Introduction |
| 1 | Scope |
| 2 | Normative references |
| 3 | Terms and definitions |
| 4 | Abbreviated terms |
| 5 | Prediction concepts |
| 5.1 | Goal of prediction |
| 5.2 | Prediction framework |
| 5.3 | Expected Level of Trust |
| 5.3.1 | Concept |
| 5.3.2 | Expected level of trust in the ONF |
| 5.3.3 | Expected level of trust in the ANF |
| 5.3.4 | ASC data in the ANF |
| 5.3.5 | Expected level of trust over sequence of application versions |
| 5.3.5.1 | Multiple versions |
| 5.3.5.2 | Version history |
| 5.3.5.3 | Original application – Version 1.0 |
| 5.3.5.4 | Version 1.1 |
| 5.3.5.5 | Version 1.2 |
| 5.3.5.6 | Version 1.3 |
| 5.3.5.7 | Version 2.0 |
| 5.4 | Principles |
| 5.4.1 | ISO/IEC 27034-1 principles |
| 5.4.2 | Appropriate investment for application security principle |
| 5.4.3 | Application security should be demonstrated principle |
| 5.5 | Prediction authorization |
| 5.5.1 | Prediction accountability |
| 5.5.2 | Forced authorization |
| 5.6 | Claims relative to the actual level of trust |
| 6 | Predictions |
| 6.1 | Prediction initiator |
| 6.2 | Prediction circumstances |
| 6.2.1 | Typical circumstance |
| 6.2.2 | Relationship to level of trust |
| 6.3 | Prediction consumer |
| 7 | Substantial changes |
| 7.1 | Definition discussion |
| 7.2 | Guidance for substantial changes risk analysis |
| 7.2.1 | General |
| 7.2.2 | Code change and static analysis |
| 7.2.3 | Architectural review |
| 7.2.4 | Deprecation of tests over time |
| 8 | Confidence |

| | |
|---|--|
| 8.1 | Confidence building blocks |
| 8.2 | Establishing confidence |
| 9 | Prediction application security rationale |
| 9.1 | Linkage to ASC |
| 9.2 | Components |
| 9.3 | Format |
| 9.3.1 | Identifiers, actors, ASCs outcomes |
| 9.3.2 | Rationale |
| 9.3.3 | Duplication of information |
| 9.3.4 | Assurance cases |
| 9.4 | Approval by ONF Committee |
| 9.5 | Use of RACI charts in description of activities, roles, and responsibilities |
| 10 | PASR audit |
| 10.1 | Auditing linkage |
| 10.2 | Auditing actual level of trust |
| 10.3 | Auditing expected level of trust |
| 10.4 | PASR quality |
| 11 | PASR Verification |
| 11.1 | Validation |
| 11.2 | Verification |
| 11.3 | Expected results |
| 11.4 | Missing state |
| 11.4.1 | Inability to generate verification measurements |
| 11.4.2 | Example |
| 12 | PASR implementation |
| 12.1 | Prediction framework |
| 12.2 | Steps to implement a PASR |
| 12.2.1 | General |
| 12.2.2 | Actor responsibilities |
| 12.3 | ONF feedback |
| 13 | Expected level of trust report |
| 13.1 | Purpose |
| 13.2 | Components |
| 13.3 | Format |
| 13.4 | History, assumptions and social history |
| Annex A (informative) Expected level of trust assurance case | |
| A.1 | Format recommendation |
| A.2 | Prediction claim |
| A.2.1 | Context |
| A.2.2 | Related consequences |
| A.2.3 | Property and limitations on its values |
| A.2.4 | Conditions and limitations on applicability |
| A.2.5 | Duration |
| A.2.6 | Uncertainty limitations |
| A.2.7 | Argument |
| A.2.8 | Justification |
| A.2.9 | Evidence |
| A.2.10 | Objective criteria |
| Annex B (informative) Comparison of ASC to PASR | |