ISO/IEC 27034-3:2018 (E)

Information technology — Application security — Part 3: Application security management process

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviated terms

5 Application Security Management Process

5.1 General
5.2 Purpose
5.3 Principles and concepts
5.3.1 General
5.3.2 Clearly communicate roles and responsibilities
5.3.3 Relationship of the ASMP with the Organizational Normative Framework (ONF)
5.3.4 Use approved tools
5.3.5 Level of Trust
5.3.6 Application‘s Targeted Level of Trust
5.3.7 Application’s Actual Level of Trust
5.3.8 Impact of this document on an application project

6 ASMP steps

6.1 Identifying the application requirements and environment
6.1.1 General
6.1.2 Purpose
6.1.3 Outcomes
6.1.4 Realization activities
6.1.5 Verification activities
6.1.6 Guidance
6.1.6.1 General
6.1.6.2 Identify the actors
6.1.6.3 Identify organizational application security specifications
6.1.6.4 Understand information flows involved by the application
6.1.6.5 Establish the application's environment
6.2 Assessing application security risks
6.2.1 General
6.2.2 Purpose
6.2.3 Outcomes
6.2.4 Realization activities
6.2.5 Verification activities
6.2.6 Guidance
6.2.6.1 Scope of the application security risk assessment
6.2.6.2 Application risk identification
6.2.6.3 Application risk analysis
6.2.6.3.1 General
6.2.6.3.2 High-level application risk analysis
6.2.6.3.3 Detailed application risk analysis
6.2.6.3.4 Techniques for detailed application risk analysis
6.2.6.3.4.1 General

6.2.6.3.4.2 Threat modelling
6.2.6.3.4.3 Threat model and attack surface review
6.2.6.4 Application risk evaluation
6.2.6.5 Application security risk assessment activities
6.2.6.6 Application security requirements
6.2.6.7 Determination of the application's Targeted Level of Trust
6.2.6.8 Application owner acceptance
6.3 Creating and maintaining the Application Normative Framework
6.3.1 General
6.3.2 Purpose
6.3.3 Outcomes
6.3.4 Realization activities
6.3.5 Verification activities
6.3.6 Guidance
6.3.6.1 General
6.3.6.2 Application Security Processes
6.3.6.3 Processes related to the ANF
6.4 Provisioning and operating the application
6.4.1 General
6.4.2 Purpose
6.4.3 Outcomes
6.4.4 Realization activities
6.4.5 Verification activities
6.4.6 Guidance
6.4.6.1 General
6.5 Auditing the security of the application
6.5.1 General
6.5.2 Purpose
6.5.3 Outcomes
6.5.4 Realization activities
6.5.5 Verification activities
6.5.6 Guidance

7 ANF elements

7.1 General
7.1.1 Purpose
7.1.2 Description
7.2 Component: Application business context
7.2.1 Purpose
7.2.2 Description
7.2.3 Contents
7.2.4 Guidance
7.3 Component: Application regulatory context
7.3.1 Purpose
7.3.2 Description
7.3.3 Contents
7.3.4 Guidance
7.4 Component: Application technological context
7.4.1 Purpose
7.4.2 Description
7.4.3 Contents
7.4.4 Guidance
7.5 Component: Application specifications
7.5.1 Purpose
7.5.2 Description
7.5.3 Contents
7.5.4 Guidance
7.6 Component: Application's actors: roles, responsibilities and qualifications
7.6.1 Purpose
7.6.2 Description
7.6.3 Contents
7.6.4 Guidance
7.6.4.1 General
7.6.4.2 Project team

7.6.4.3 Operation team
7.7 Component: Selected ASCs for the application's life cycle stages
7.7.1 Purpose
7.7.2 Description
7.7.3 Contents
7.7.4 Guidance
7.8 Processes related to the security of the application
7.8.1 Purpose
7.8.2 Description
7.8.3 Contents
7.8.4 Guidance
7.9 Component: Application life cycle
7.9.1 Purpose
7.9.2 Description
7.9.3 Contents
7.9.4 Guidance
7.10 Information involved by the application
7.10.1 Purpose
7.10.2 Description
7.10.3 Contents
7.10.4 Guidance

Annex A (informative) Guidance text related to the ASMP step: (6.4) Realizing and operating the application

A.1 Guidance
A.1.1 General
A.1.2 Static analysis
A.1.3 Dynamic program analysis
A.1.4 Fuzz testing
A.1.5 Exception process
A.1.5.1 General
A.1.5.2 Exception process
A.1.5.3 Change management process
A.1.5.4 Feedback process

Page count: 47