ISO/IEC 27034-5:2017-10 (E)

Information technology - Security techniques - Application security - Part 5: Protocols and application security controls data structure

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Abbreviated terms 2

5 Application Security Control Structure 2
5.1 General 2
5.2 ASC information requirements 2
5.2.1 Overview 2
5.2.2 Integrity assurance 4
5.2.3 Multilingual/multiregional data representation 4
5.2.4 ASC information requirements 5
5.3 ASC data structure recommendations 14
5.3.1 General 14
5.3.2 Exchange 14
5.3.3 Self-containedness 14

6 Application Security Life Cycle Reference Model 14
6.1 General 14
6.2 Application Management Layer 16
6.2.1 General 16
6.2.2 Initiating 16
6.2.3 Planning 16
6.2.4 Executing 17
6.2.5 Monitoring and controlling 17
6.2.6 Closing 18
6.3 Application provisioning and operation layer 18
6.3.1 General 18
6.3.2 Preparation: Initiating 18
6.3.3 Preparation: Plan 19
6.3.4 Outsourcing: Realization 19
6.3.5 Outsourcing: Transition 19
6.3.6 Development: Inception 20
6.3.7 Development: Elaboration 20
6.3.8 Development: Construction 20
6.3.9 Acquisition: Plan 21
6.3.10 Acquisition: Close 21
6.3.11 Transition: Plan 21
6.3.12 Transition: Development 21
6.3.13 Transition: Test 22
6.3.14 Utilization: Utilization 22
6.3.15 Utilization: Maintenance 23
6.3.16 Archival: Archival 23
6.3.17 Destruction: Destruction 24

6.4 Infrastructure management 25
6.4.1 General 25
6.4.2 Establishment of the infrastructure 25
6.4.3 Maintenance of the infrastructure 25
6.5 Application audit 26
6.5.1 General 26
6.5.2 Initiating the audit 26
6.5.3 Prepare the audit 27

6.5.4 Conduct the audit 27
6.5.5 Report 28
6.5.6 Complete the audit 28
6.5.7 Follow-up 28
6.6 Roles 29

7 ASC Package 31

Bibliography 33