

ISO/IEC 27034-6:2016-10 (E)

Information technology - Security techniques - Application security - Part 6: Case studies

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	1
5	Security guidance for specific applications	1
5.1	General	1
5.2	ASC example: Java code revision for mobile applications	2
5.2.1	General	2
5.2.2	Purpose	2
5.2.3	Context	2
5.2.4	ORGANISATION Information classification guidelines	2
5.2.5	Levels of trust included in the ORGANISATION ASC Library	2
5.2.6	Outcome	3
5.2.7	ORGANISATION stakeholders involved in these ASCs	4
5.2.8	Descriptions of sample ASCs	6
5.3	Case study: Developing ASCs to address the issue of privacy for two countries	19
5.3.1	General	19
5.3.2	Purpose	19
5.3.3	Context	19
5.4	Case study: Integration of third-party ASCs	21
5.4.1	General	21
5.4.2	Purpose	21
5.4.3	Context	21
5.5	Case study: Using the ASLCRM to facilitate implementation of ASCs by different development groups inside an organization	24
5.5.1	General	24
5.5.2	Purpose	24
5.5.3	Context	24
5.6	Case study: Implementation of third-party ASCs in a secure development life cycle process	26
5.6.1	General	26
5.6.2	Purpose	26
5.6.3	Context	26
5.6.4	Preparation phase (1.00)	27
5.6.5	Requirements phase (2.00)	30
5.6.6	Design phase (3.00)	31
5.6.7	Implementation phase (4.00)	34
5.6.8	Verification phase (5.00)	36
5.6.9	Release phase (6.00)	37
5.6.10	Sustainment, support and servicing phase (7.00)	38
Annex A (informative)	XML examples for case studies in 5.2	41
Bibliography		70