

ISO/IEC 27034-2:2015-08 (E)

Information technology - Security techniques - Application security - Part 2: Organization normative framework

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	1
5	Organization Normative Framework	2
5.1	General	2
5.2	Purpose	2
5.3	Principles	2
5.4	ONF Management Process	2
5.4.1	General	2
5.4.2	Use of RACI charts in description of activities, roles and responsibilities	4
5.4.3	Establishing the ONF committee	5
5.4.4	Designing the ONF	6
5.4.5	Implementing the ONF	8
5.4.6	Monitoring and reviewing the ONF	10
5.4.7	Improving the ONF	11
5.4.8	Auditing the ONF	13
5.5	ONF Elements	15
5.5.1	General	15
5.5.2	Business context component	16
5.5.3	Regulatory context component	17
5.5.4	Technological context component	18
5.5.5	Application specifications repository	19
5.5.6	Roles, responsibilities and qualifications repository	20
5.5.7	Organization ASC Library	21
5.5.8	Application Security Control	23
5.5.9	Application Security Life Cycle Reference Model	26
5.5.10	Application Security Life Cycle Model	32
5.5.11	Application Security Management Process	33
5.5.12	Application Security Risk Analysis Process	34
5.5.13	Application Security Verification Process	36
Application Security and its ONF in an existing organization		42
Bibliography		52