ISO/IEC TS 33072:2016-07 (E)

Information technology - Process assessment - Process capability assessment model for information security management

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Overview of the Process Assessment Model 2
4.1 Introduction to Overview 2
4.2 Structure of the Process Assessment Model 3
4.2.1 Processes 3
4.2.2 Process dimension 4
4.2.3 Capability dimension 4
4.3 Assessment Indicators 6
4.3.1 Process Capability Indicators 7
4.3.2 Process Performance Indicators 8
4.4 Measuring process capability 9

5 The process dimension and process performance indicators (Level 1) 10
5.1 General 10
5.2 ORG.1 Asset management 11
5.3 TEC.01 Capacity management 12
5.4 TEC.02 Change management 13
5.5 COM.01 Communication management 13
5.6 TEC.03 Configuration management 14
5.7 COM.02 Documentation management 15
5.8 ORG.2 Equipment management 17
5.9 ORG.3 Human resource employment management 18
5.10 COM.03 Human resource management 19
5.11 COM.04 Improvement 20
5.12 TEC.04 Incident management 21
5.13 ORG.4 Infrastructure and work environment 21
5.14 COM.05 Internal audit 22
5.15 TOP.1 Leadership 23
5.16 COM.06 Management review 24
5.17 COM.07 Non-conformity management 25
5.18 COM.09 Operational implementation and control 26
5.19 COM.08 Operational planning 27
5.20 COM.10 Performance evaluation 29
5.21 TEC.05 Product/service release 30
5.22 TEC.08 Product/Service/System requirements 31
5.23 COM.11 Risk and opportunity management 32
5.24 TEC.06 Service availability management 33
5.25 TEC.07 Service continuity management 34
5.26 ORG.5 Supplier management 34
5.27 TEC.09 Technical data preservation and recovery 35

6 Process capability indicators 36

6.1 Introduction 36
6.2 Process capability levels and process attributes 36
6.2.1 Process capability Level 0: Incomplete process 36
6.2.2 Process capability Level 1: Performed process 36
6.2.3 Process capability Level 2: Managed process 37
6.2.4 Process capability Level 3: Established process 42
6.2.5 Process capability Level 4: Predictable process 46
6.2.6 Process capability Level 5: Innovating process 51
6.3 Related processes for process attributes 55

Annex A (informative) Conformity of the process assessment model 57

A.1 Introduction 57
A.2 Requirements for process assessment models 57
A.2.1 Introduction 57
A.2.2 Process assessment model scope 57
A.2.3 Requirements for process assessment models 58
A.2.4 Assessment indicators 58
A.2.5 Mapping process assessment models to process reference models 59
A.2.6 Expression of assessment results 61

Annex B (informative) Input and output characteristics 62

B.1 General 62
B.2 Generic input and outputs 63
B.3 Specific inputs and outputs 67

C.1 Associations of base practices with requirements 98
C.2 Associations of requirements with base practices 136
C.3 Base practices that have no associated requirements 180

Bibliography 183