ISO/IEC 27004:2009-12 (E)

Information technology - Security techniques - Information security management - Measurement

Contents

Page

Foreword v

0 Introduction vi
0.1 General vi
0.2 Management overview vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Structure of this International Standard 3

5 Information security measurement overview 4
5.1 Objectives of information security measurement 4
5.2 Information Security Measurement Programme 5
5.3 Success factors 6
5.4 Information security measurement model 6
5.4.1 Overview 6
5.4.2 Base measure and measurement method 7
5.4.3 Derived measure and measurement function 9
5.4.4 Indicators and analytical model 10
5.4.5 Measurement results and decision criteria 11

6 Management responsibilities 12
6.1 Overview 12
6.2 Resource management 13
6.3 Measurement training, awareness, and competence 13

7 Measures and measurement development 13
7.1 Overview 13
7.2 Definition of measurement scope 13
7.3 Identification of information need 14
7.4 Object and attribute selection 14
7.5 Measurement construct development 15
7.5.1 Overview 15
7.5.2 Measure selection 15
7.5.3 Measurement method 15
7.5.4 Measurement function 16
7.5.5 Analytical model 16
7.5.6 Indicators 16
7.5.7 Decision criteria 16
7.5.8 Stakeholders 17
7.6 Measurement construct 17
7.7 Data collection, analysis and reporting 17
7.8 Measurement implementation and documentation 18

8 Measurement operation 18
8.1 Overview 18
8.2 Procedure integration 18

8.3 Data collection, storage and verification 19

9 Data analysis and measurement results reporting 19
9.1 Overview 19
9.2 Analyse data and develop measurement results 19
9.3 Communicate measurement results 20

10 Information Security Measurement Programme Evaluation and Improvement 20
10.1 Overview 20
10.2 Evaluation criteria identification for the Information Security Measurement Programme .. 21
10.3 Monitor, review, and evaluate the Information Security Measurement Programme 21
10.4 Implement improvements 21

Annex A (informative) Template for an information security measurement construct 22

Annex B (informative) Measurement construct examples 24

Bibliography 55