# ISO 28003:2007-08 (E)

## Security management systems for the supply chain - Requirements for bodies providing audit and certification of supply chain secur ity management systems

## Contents

Page


Foreword ..... iv

Introduction ..... v

1 Scope ..... 1

2 Normative references ..... 1

3 Terms and definitions ..... 2

4 Principles for certification bodies ..... 2
4.1 General ..... 2
4.2 Impartiality ..... 3
4.3 Competence ..... 4
4.4 Responsibility ..... 4
4.5 Openness ..... 4
4.6 Confidentiality ..... 4
4.7 Resolution of complaints ..... 4

5 General requirements ..... 4
5.1 Legal and contractual matters ..... 4
5.2 Management of impartiality ..... 5
5.3 Liability and financing ..... 6

6 Structural requirements ..... 6
6.1 Organizational structure and top management ..... 6
6.2 Committee for safeguarding impartiality ..... 7

7 Resource requirements ..... 8
7.1 Competence of management and personnel ..... 8
7.2 Personnel involved in the certification activities ..... 8
7.3 Use of external auditors and external technical experts ..... 10
7.4 Personnel records ..... 11
7.5 Outsourcing ..... 12

8 Information requirements ..... 13
8.1 Publicly accessible information ..... 13
8.2 Certification documents ..... 13
8.3 Directory of certified clients ..... 14
8.4 Reference to certification and use of marks ..... 14
8.5 Confidentiality ..... 14
8.6 Information exchange between a certification body and its clients ..... 15

9 Process requirements ..... 16
9.1 General requirements applicable to any audit ..... 16
9.2 Initial audit and certification ..... 18
9.3 Surveillance activities ..... 23
9.4 Recertification ..... 25
9.5 Special audits ..... 27
9.6 Suspending, withdrawing or reducing scope of certification ..... 27
9.7 Appeals ..... 28

9.8 Complaints ..... 28
9.9 Records on applicants and clients ..... 29

10 Management system requirements for certification bodies ..... 30
10.1 Option 1 -- Management system requirements in accordance with ISO 9001 ..... 30
10.2 Option 2 -- General management system requirements ..... 30

Annex A (informative) Guide for process to determine auditor time ..... 34

Annex B (normative) Criteria for auditing organizations with multiple sites ..... 36

Annex C (normative) Auditor education, work and audit experience and training durations ..... 40

Annex D (normative) Auditor competence requirements ..... 41

Bibliography ..... 43