ISO 37003:2025-05 (E)

Fraud control management systems - Guidance for organizations managing the risk of fraud

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Context of the organization **8**
4.1 Understanding the organization and its context 8
4.2 Understanding the needs and expectations of interested parties 8
4.3 Determining the scope of the fraud control management system (FCMS) 9
4.4 Fraud control management system (FCMS) 9
4.5 Fraud risk assessment 9
4.5.1 General 9
4.5.2 Collaboration with other risk management functions 10

5 Leadership **10**
5.1 Leadership and commitment 10
5.1.1 Governing body 10
5.1.2 Top management 10
5.2 Fraud control policy 11
5.3 Roles, responsibilities and authorities 11
5.3.1 General 11
5.3.2 Delegated decision-making to managers and organizational functions 11
5.3.3 Fraud control function 11
5.3.4 Information security management system function 12
5.3.5 Internal audit function 12

6 Planning **13**
6.1 Actions to address risks and opportunities 13
6.1.1 General 13
6.2 Fraud control objectives and planning to achieve them 13
6.3 Planning of changes 14

7 Support **14**
7.1 Resources 14
7.1.1 General 14
7.1.2 Information security management system function 14
7.2 Competence 14
7.2.1 General 14
7.2.2 Employment process 15
7.3 Awareness 15
7.3.1 Awareness of personnel 15
7.3.2 Training for personnel 16
7.3.3 Training for business associates 16
7.3.4 Awareness and training programmes 16
7.4 Communication 17
7.4.1 General 17
7.4.2 Promoting the FCMS 17
7.5 Documented information 17
7.5.1 General 17

7.5.2 Creating and updating documented information 18
7.5.3 Control of documented information 18
7.5.4 Record keeping and confidentiality of information 18

8 Operation 19
8.1 Operational planning and control 19
8.2 Preventing fraud 20
8.2.1 General 20
8.2.2 Developing and promoting an effective integrity framework 20
8.2.3 Managing conflicts of interest 21
8.2.4 Internal controls and the internal control environment 21
8.2.5 Pressure testing the internal control system 22
8.2.6 Managing performance-based targets 22
8.2.7 Personnel screening 23
8.2.8 Screening and management of business associates 23
8.2.9 Preventing technology-enabled fraud 24
8.2.10 Physical security and asset management 25
8.3 Detecting fraud 25
8.3.1 General 25
8.3.2 Post-transactional review 25
8.3.3 Analysis of management accounting reports 25
8.3.4 Identification of early warning indicators 26
8.3.5 Data analytics 26
8.3.6 Fraud reporting 27
8.3.7 Artificial intelligence systems 27
8.3.8 Complaint management 28
8.3.9 Exit interviews 28
8.4 Responding to fraud events 28
8.4.1 General 28
8.4.2 Immediate actions in response to discovery of fraud 28
8.4.3 Digital evidence first response 29
8.4.4 Investigation of a detected fraud event 29
8.4.5 Consideration of grievances 29
8.4.6 Disciplinary procedures 29
8.4.7 Separation of investigation and decision-making processes 29
8.4.8 Crisis management following discovery of a fraud event 29
8.4.9 Internal reporting and escalation 30
8.4.10 Fraud event register 30
8.4.11 Analysis and reporting of fraud events 30
8.4.12 External reporting 31
8.4.13 Recovery of stolen funds or property 31
8.4.14 Responding to fraud events involving business associates 32
8.4.15 Insuring against fraud events 32
8.4.16 Assessing internal controls, systems and processes post-detection of a fraud event 32
8.4.17 Impact of fraud on other interested parties 33
8.4.18 Disruption of fraud 33

9 Performance evaluation 34
9.1 Monitoring, measurement, analysis and evaluation 34
9.2 Internal audit 34
9.2.1 General 34
9.2.2 Internal audit programme 35
9.3 External audit 35
9.4 Management review 36
9.4.1 General 36
9.4.2 Management review inputs 36
9.4.3 Management review results 36

10 Improvement 36
10.1 Continual improvement 36
10.2 Nonconformity and corrective action 36

Annex A (informative) **Examples of fraud risks impacting global entities 38**

Annex B (informative) **Models for fraud prevention — Guidance 41**

Bibliography 45