ISO 37301:2021 (E)

Compliance management systems — Requirements with guidance for use

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Context of the organization

- 4.1 Understanding the organization and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of the compliance management system
- 4.4 Compliance management system
- 4.5 Compliance obligations
- 4.6 Compliance risk assessment

5 Leadership

- 5.1 Leadership and commitment
- 5.1.1 Governing body and top management
- 5.1.2 Compliance culture
- 5.1.3 Compliance governance
- 5.2 Compliance policy
- 5.3 Roles, responsibilities and authorities
- 5.3.1 Governing body and top management
- 5.3.2 Compliance function
- 5.3.3 Management
- 5.3.4 Personnel

6 Planning

- 6.1 Actions to address risks and opportunities
- 6.2 Compliance objectives and planning to achieve them
- 6.3 Planning of changes

7 Support

- 7.1 Resources
- 7.2 Competence
- 7.2.1 General
- 7.2.2 Employment process
- 7.2.3 Training
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information
- 7.5.1 General
- 7.5.2 Creating and updating documented information
- 7.5.3 Control of documented information

8 Operation

- 8.1 Operational planning and control
- 8.2 Establishing controls and procedures
- 8.3 Raising concerns
- 8.4 Investigation processes

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation
9.1.1 General
9.1.2 Sources of feedback on compliance performance
9.1.3 Development of indicators
9.1.4 Compliance reporting
9.1.5 Record-keeping
9.2 Internal audit
9.2.1 General
9.2.2 Internal audit programme
9.3 Management review
9.3.1 General
9.3.2 Management review inputs
9.3.3 Management review results

10 Improvement

10.1 Continual improvement
10.2 Nonconformity and corrective action

Annex A (informative) Guidance for the use of this document

A.1 Background and Scope
A.1.1 General
A.1.2 Scope
A.2 Normative references
A.3 Terms and definitions
A.4 Context of the organization
A.4.1 Understanding the organization and its context
A.4.2 Understanding the needs and expectations of interested parties
A.4.3 Determining the scope of the compliance management system
A.4.4 Compliance management system
A.4.5 Compliance obligations
A.4.6 Compliance risk assessment
A.5 Leadership
A.5.1 Leadership and commitment
A.5.1.1 Governing body and top management
A.5.1.2 Compliance culture
A.5.1.3 Compliance governance
A.5.2 Compliance policy
A.5.3 Roles, responsibilities and authorities
A.5.3.1 Governing body and top management
A.5.3.2 Compliance function
A.5.3.3 Management
A.5.3.4 Personnel
A.6 Planning
A.6.1 Actions to address risks and opportunities
A.6.2 Compliance objectives and planning to achieve them
A.7 Support
A.7.1 Resources
A.7.2 Competence
A.7.2.1 General
A.7.2.2 Employment process
A.7.2.3 Training
A.7.3 Awareness
A.7.4 Communication
A.7.5 Documented information
A.7.5.1 General
A.7.5.2 Creating and updating documented information
A.7.5.3 Control of documented information
A.8 Operation
A.8.1 Operational planning and control
A.8.2 Establishing controls and procedures
A.8.3 Raising concerns
A.8.4 Investigation processes

A.9 Performance evaluation
A.9.1 Monitoring, measurement, analysis and evaluation
A.9.1.1 General
A.9.1.2 Sources of feedback on compliance performance
A.9.1.3 Development of indicators
A.9.1.4 Compliance reporting
A.9.1.5 Record-keeping
A.9.2 Internal audit
A.9.3 Management review
A.10 Improvement
A.10.1 Continual improvement
A.10.2 Nonconformity and corrective action

Page count: 40