

# Table of content

|           |                      |                                                                       |
|-----------|----------------------|-----------------------------------------------------------------------|
| <b>8</b>  | <b>Foreword</b>      |                                                                       |
| <b>12</b> | <b>Abbreviations</b> |                                                                       |
| <b>16</b> | <b>1</b>             | <b>Basic principles and general framework</b>                         |
| 17        | 1.1                  | Definition of the term 'compliance'                                   |
| 18        | 1.2                  | Legal framework for compliance in organisations                       |
| 19        | 1.2.1                | Responsibility of organisations in the international arena            |
| 20        | 1.2.2                | Responsibility of organisations at the national level                 |
| 20        | 1.2.3                | Responsibility for compliance in Austria                              |
| 21        | 1.3                  | Compliance as a tool of strategic management                          |
| 21        | 1.3.1                | Definition of management systems                                      |
| 24        | 1.3.2                | Compliance Management Systems                                         |
| 25        | 1.4                  | Distinction between corporate governance – ICS – RMS – CMS            |
| 26        | 1.4.1                | Corporate governance                                                  |
| 27        | 1.4.2                | Internal control system (ICS)                                         |
| 29        | 1.4.3                | Risk management system (RMS)                                          |
| 29        | 1.4.4                | Compliance management system (CMS)                                    |
| 30        | 1.5                  | Standardisation of management systems in accordance with ISO          |
| 31        | 1.6                  | Certification                                                         |
| 32        | 1.6.1                | Importance of the certification of a CMS                              |
| 34        | 1.6.2                | Certification under ISO                                               |
| <b>36</b> | <b>2</b>             | <b>A CMS in accordance with ISO 19600 at a glance</b>                 |
| 38        | 2.1                  | Positioning of ISO 19600 as a best-practise approach                  |
| 38        | 2.1.1                | Positioning of ISO 19600 compared to legal requirements               |
| 42        | 2.1.2                | ISO 19600 in comparison with selected management tools                |
| 48        | 2.2                  | Approach for the implementation of a CMS in accordance with ISO 19600 |
| 51        | 2.2.1                | PLAN – Preparation                                                    |
| 53        | 2.2.2                | DO – Implementation                                                   |
| 54        | 2.2.3                | CHECK – Verification                                                  |
| 54        | 2.2.4                | ACT – Improvement                                                     |
| <b>56</b> | <b>3</b>             | <b>Elements of ISO 19600 – Compliance Management Systems</b>          |
| 57        | 3.1                  | Introduction                                                          |
| 58        | 3.2                  | Area of application of the ISO 19600 standard                         |
| 59        | 3.3                  | Definitions in accordance with ISO 19600                              |
| 75        | 3.4                  | Context of the organisation                                           |
| 75        | 3.4.1                | Understanding the organisation and its context                        |
| 79        | 3.4.2                | Understanding the needs and expectations of interested parties        |
| 82        | 3.4.3                | Determining the scope of the compliance management systems            |
| 83        | 3.4.4                | CMS and principles of good governance                                 |
| 85        | 3.4.5                | Compliance obligations                                                |
| 88        | 3.4.6                | Identification, analysis and evaluation of compliance risks           |
| 92        | 3.5                  | Leadership                                                            |
| 92        | 3.5.1                | Leadership and commitment                                             |
| 95        | 3.5.2                | Compliance policy                                                     |
| 99        | 3.5.3                | Organisational roles, responsibilities and authorities                |
| 105       | 3.5.4                | Management responsibility                                             |
| 106       | 3.5.5                | Employee responsibility                                               |

|            |          |                                                                             |
|------------|----------|-----------------------------------------------------------------------------|
| 110        | 3.6      | Planning                                                                    |
| 110        | 3.6.1    | Actions to address compliance risks                                         |
| 112        | 3.6.2    | Compliance objectives and planning to achieving them                        |
| 115        | 3.7      | Support                                                                     |
| 115        | 3.7.1    | Resources                                                                   |
| 117        | 3.7.2    | Competence and training                                                     |
| 121        | 3.7.3    | Awareness                                                                   |
| 123        | 3.7.4    | Communication                                                               |
| 128        | 3.7.5    | Documented information                                                      |
| 129        | 3.8      | Operation                                                                   |
| 129        | 3.8.1    | Operational planning and control                                            |
| 130        | 3.8.2    | Establishing controls and procedures                                        |
| 133        | 3.8.3    | Outsourced processes                                                        |
| 140        | 3.9      | Performance evaluation                                                      |
| 140        | 3.9.1    | Monitoring, measurement, analysis and evaluation                            |
| 146        | 3.9.2    | Audits                                                                      |
| 147        | 3.9.3    | Management review                                                           |
| 148        | 3.10     | Improvement                                                                 |
| 148        | 3.10.1   | Nonconformity, non-compliance and corrective measures                       |
| 151        | 3.10.2   | Escalation                                                                  |
| 155        | 3.10.3   | Continual improvement                                                       |
| <b>160</b> | <b>4</b> | <b>Guide for small and medium-sized enterprises (SMEs)</b>                  |
| 162        | 4.1      | Compliance-relevant characteristics of SMEs                                 |
| 164        | 4.2      | Implementation and configuration of compliance management in the SME sector |
| 173        | 4.3      | Conclusion                                                                  |
| <b>176</b> | <b>5</b> | <b>Advanced concepts</b>                                                    |
| 177        | 5.1      | Change management as a management tool                                      |
| 178        | 5.1.1    | Definition of change management                                             |
| 179        | 5.1.2    | Reasons/drivers for change management processes                             |
| 181        | 5.1.3    | Factors influencing change management processes                             |
| 189        | 5.1.4    | Three-phase approach to changes according to Lewin                          |
| 191        | 5.1.5    | Leading Change – The 8-Step Model by John Kotter                            |
| 194        | 5.1.6    | Change management and a CMS in accordance with ISO 19600                    |
| 196        | 5.2      | Organisational culture as a management tool                                 |
| 196        | 5.2.1    | Influences on organisational cultures                                       |
| 198        | 5.2.2    | Characteristics of organisational cultures                                  |
| 200        | 5.2.3    | The cultural model according to Schein                                      |
| 202        | 5.2.4    | Effect and function of organisational cultures                              |
| 203        | 5.2.5    | Measurement of organisational cultures – the model by Denison               |
| 209        | 5.2.6    | Organisational culture and a CMS in accordance with ISO 19600               |
| 210        | 5.3      | Risk management                                                             |
| 211        | 5.3.1    | A brief history of risk management                                          |
| 212        | 5.3.2    | Risk management systems at a glance                                         |
| 216        | 5.3.3    | ERM – a holistic, organisation-wide risk management system                  |
| 225        | 5.3.4    | ISO 31000 Risk Management                                                   |
| 228        | 5.3.5    | Risk management and a CMS in accordance with ISO 19600                      |
| <b>230</b> | <b>6</b> | <b>Summary and forecast</b>                                                 |
| <b>232</b> |          | <b>Bibliography</b>                                                         |
| <b>243</b> |          | <b>The author</b>                                                           |

# List of figures

|     |           |                                                                           |
|-----|-----------|---------------------------------------------------------------------------|
| 28  | Figure 1  | COSO Internal Control – Integrated Framework                              |
| 34  | Figure 2  | Audit process in accordance with ISO/IEC 17021                            |
| 49  | Figure 3  | ISO 19600 in the Deming cycle of continuous improvement                   |
| 76  | Figure 4  | PESTLE analysis of the external environment                               |
| 79  | Figure 5  | Internal determinants of an organisation according Huczynski/<br>Buchanan |
| 80  | Figure 6  | Stakeholders/interested parties                                           |
| 91  | Figure 7  | Risk Matrix                                                               |
| 93  | Figure 8  | Level and characteristics of a code of conduct                            |
| 96  | Figure 9  | Compliance in support of organisational goals                             |
| 97  | Figure 10 | Means of implementing compliance policy                                   |
| 107 | Figure 11 | Components of the capacity to act                                         |
| 108 | Figure 12 | The Fraud Triangle and approaches to prevention according to<br>Grüninger |
| 114 | Figure 13 | Indicators for CMS objectives according to Johnson/Søreide                |
| 122 | Figure 14 | Value orientation of CMS according to Grüninger                           |
| 125 | Figure 15 | Overview of communication according to Mast/Maletzke                      |
| 138 | Figure 16 | Sequence of a monitoring procedure                                        |
| 156 | Figure 17 | DMAIC cycle of continuous improvement                                     |
| 161 | Figure 18 | EU definition of SME                                                      |
| 174 | Figure 19 | Approaches to compliance management according to Saitz/Tempel/<br>Brühl   |
| 179 | Figure 20 | Change management as a method/operating principle                         |
| 180 | Figure 21 | Reasons/drivers for change management processes according to<br>Kotter    |
| 182 | Figure 22 | 7-S Model according to Pascal / Athos                                     |
| 184 | Figure 23 | Promotors and destructors according to Ladwig/Domsch                      |
| 185 | Figure 24 | The complexity of relations according to Neuburger                        |
| 186 | Figure 25 | Common symptoms of resistance according to Doppler/Lauterburg             |
| 187 | Figure 26 | Selected areas of action for resistance according to Reiss                |
| 188 | Figure 27 | Acceptance-promoting aspects of change processes according to<br>Reiss    |
| 189 | Figure 28 | Phase diagram of changes according to Lewin                               |
| 192 | Figure 29 | 8-step model for changes according to Kotter                              |
| 197 | Figure 30 | Factors of organisational culture according to Sackmann                   |
| 200 | Figure 31 | Cultural box model according to Thomas                                    |
| 201 | Figure 32 | Cultural levels according to Schein                                       |
| 204 | Figure 33 | Framework organisational culture/effectiveness according to<br>Denison    |
| 207 | Figure 34 | Organisational cultures according to Denison                              |
| 208 | Figure 35 | Corporate culture and effectiveness                                       |
| 214 | Figure 36 | Building-blocks of a risk management system                               |
| 217 | Figure 37 | COSO ERM Framework                                                        |
| 220 | Figure 38 | Risk matrix                                                               |
| 225 | Figure 39 | Connecting elements of risk framework according ISO 3100:2009             |
| 227 | Figure 40 | Risk management process ISO 31000:2009                                    |

# List of tables

|     |          |                                                                   |
|-----|----------|-------------------------------------------------------------------|
| 32  | Table 1  | Types of system audits                                            |
| 39  | Table 2  | Guideline UK Bribery Act vs. ISO 19600                            |
| 40  | Table 3  | US Sentencing Guideline Manual Chapter 8(B) vs. ISO 19600         |
| 41  | Table 4  | ICC Anti-Corruption Policy vs. ISO 19600                          |
| 44  | Table 5  | Kotter Change Management Model vs. ISO 19600                      |
| 46  | Table 6  | Denison effectiveness model vs. ISO 19600                         |
| 47  | Table 7  | COSO ERM vs. ISO 19600                                            |
| 90  | Table 8  | Probability scale                                                 |
| 90  | Table 9  | Specimen risk map                                                 |
| 124 | Table 10 | Information and communication needs according to Bruhn            |
| 127 | Table 11 | Classification of means of communication according to Vahs/Weiand |
| 222 | Table 12 | Structure of key risk indicators (KRI)                            |