# Contents

<table>
<thead>
<tr>
<th>Acknowledgments</th>
<th>xi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>xiii</td>
</tr>
</tbody>
</table>

1. **Governance Overview—How Do We Do It? What Do We Get Out of It?**

   1.1 What Is It? 1
   1.2 Back to Basics 2
   1.3 Origins of Governance 3
   1.4 Governance Definition 5
   1.5 Information Security Governance 5
   1.6 Six Outcomes of Effective Security Governance 6
   1.7 Defining Information, Data, Knowledge 7
   1.8 Value of Information 7

2. **Why Governance?** 9

   2.1 Benefits of Good Governance 11
      2.1.1 Aligning Security with Business Objectives 11
      2.1.2 Providing the Structure and Framework to Optimize Allocations of Limited Resources 12
      2.1.3 Providing Assurance that Critical Decisions are Not Based onFaulty Information 13
      2.1.4 Ensuring Accountability for Safeguarding Critical Assets 13
      2.1.5 Increasing Trust of Customers and Stakeholders 14
      2.1.6 Increasing the Company’s Worth 14
      2.1.7 Reducing Liability for Information Inaccuracy or Lack of Due Care in Protection 14
      2.1.8 Increasing Predictability and Reducing Uncertainty of Business Operations 15
   2.2 A Management Problem 15
11. Sample Strategy Development 99
  11.1 The Process 100

12. Implementing Strategy 109
  12.1 Action Plan Intermediate Goals 109
  12.2 Action Plan Metrics 110
  12.3 Reengineering 110
  12.4 Inadequate Performance 110
  12.5 Elements of Strategy
    12.5.1 Policy Development 111
    12.5.2 Standards 116
  12.6 Summary 125

13. Security Program Development Metrics 127
  13.1 Information Security Program Development Metrics 127
  13.2 Program Development Operational Metrics 129

  14.1 Management Metrics 132
  14.2 Security Management Decision Support Metrics 132
  14.3 CISO Decisions 134
    14.3.1 Strategic Alignment—Aligning Security Activities in Support of Organizational Objectives 134
    14.3.2 Risk Management—Executing Appropriate Measures to Manage Risks and Potential Impacts to an Acceptable Level 137
    14.3.3 Metrics for Risk Management 138
    14.3.4 Assurance Process Integration 141
    14.3.5 Value Delivery—Optimizing Investments in Support of the Organization’s Objectives 142
    14.3.6 Resource Management—Using Organizational Resources Efficiently and Effectively 144
    14.3.7 Performance Measurement—Monitoring and Reporting on Security Processes to Ensure that Organizational Objectives are Achieved 145
  14.4 Information Security Operational Metrics 145
    14.4.1 IT and Information Security Management 145
    14.4.2 Compliance Metrics 146

15. Incident Management and Response Metrics 155
  15.1 Incident Management Decision Support Metrics 156
    15.1.1 Is It Actually and Incident? 156
15.1.2 What Kind of Incident Is It? 157
15.1.3 Is It a Security Incident? 157
15.1.4 What Is the Security Level? 157
15.1.5 Are there Multiple Events and/or Impacts 158
15.1.6 Will an Incident Need Triage? 158
15.1.7 What Is the Most Effective Response? 158
15.1.8 What Immediate Actions Must be Taken? 158
15.1.9 Which Incident Response Teams and Other Personnel Must be Mobilized? 159
15.1.10 Who Must be Notified? 159
15.1.11 Who Is in Charge? 159
15.1.12 Is It Becoming a Disaster? 159

16. Conclusion 161

APPENDIX A. SABSA Business Attributes and Metrics 163

APPENDIX B. Cultural Worldviews 181

Heirarchists 181
Egalitarians 181
Individualists 182
Fatalists 182

Index 185