

IT Strategic and Operational Controls

JOHN KYRIAZOGLOU



IT Governance Publishing

CONTENTS

Chapter 1: IT ORGANISATION CONTROLS	1
1.1 Scope	1
1.2 Purpose and main types of IT organisation controls...	2
1.3 IT department functional description controls	3
1.4 IT organisation controls	22
1.5 IT vision, mission and values statements	29
1.6 IT governance and control frameworks	31
1.7 Monitoring and review controls	41
1.8 IT organisation performance measures	44
1.9 Review and audit tools and techniques	46
1.10 Conclusion	54
1.11 Review questions	56
Chapter 2: IT ADMINISTRATION CONTROLS	61
2.1 Scope	61
2.2 Purpose and main types of IT administration controls	62
2.3 IT standards, policies and procedures	63
2.4 IT budget	65
2.5 IT asset controls	67
2.6 IT personnel management controls	68
2.7 IT purchasing controls	83
2.8 IT office administration controls	94
2.9 Monitoring and review controls	99
2.10 IT administration performance measures	100
2.11 Review and audit tools and techniques	101
2.12 Conclusion	111
2.13 Review questions	112
Chapter 3: ENTERPRISE ARCHITECTURE CONTROLS	117
3.1 Scope	117

Contents

3.2 Purpose and main types of Enterprise Architecture controls	118
3.3 Enterprise Architecture (EA) description controls	120
3.4 Management plan for designing and implementing an Enterprise Architecture (EA) framework	128
3.5 Enterprise Architecture development roles	132
3.6 Formulating and documenting the Enterprise Architecture elements	135
3.7 Other Enterprise Architecture business-related controls	147
3.8 Enterprise Architecture IT-related controls	150
3.9 Monitoring and review controls	150
3.10 Review and audit tools and techniques	151
3.11 Conclusion	160
3.12 Review questions	163
Chapter 4: IT STRATEGIC CONTROLS	167
4.1 Scope	167
4.2 Characteristics of strategy	167
4.3 Purpose and main types of IT strategic controls	171
4.4 IT strategic process controls	173
4.5 IT strategy implementation controls	190
4.6 IT strategic performance management controls	197
4.7 Monitoring and review controls	204
4.8 Review and audit tools and techniques	208
4.9 Conclusion	218
4.10 Review questions	221
Chapter 5: SYSTEM DEVELOPMENT CONTROLS	225
5.1 Scope	225
5.2 Purpose and main types of system development controls	226
5.3 Application systems development process controls	227
5.4 System development quality controls	253

5.5 Change management controls	255
5.6 Systems development personnel controls	259
5.7 Monitoring and review controls	262
5.8 Systems development performance measures	263
5.9 Review and audit tools and techniques	264
5.10 Conclusion	275
5.11 Review questions	276
Chapter 6: IT SECURITY CONTROLS	281
6.1 Scope	281
6.2 Purpose and main types of IT security controls	282
6.3 IT security governance guidelines, standards and legal frameworks	284
6.4 IT security plans and policies	290
6.5 IT security procedures and practices	304
6.6 Specialised IT security hardware and software protection controls	316
6.7 Evaluation and monitoring controls of IT security	319
6.8 IT security performance measures	324
6.9 Review and audit tools and techniques	326
6.10 Conclusion	335
6.11 Review questions	336
Chapter 7: DATA CENTRE OPERATIONAL AND SUPPORT CONTROLS	341
7.1 Scope	341
7.2 Purpose and main types of data centre operational and support controls	342
7.3 Data centre design and infrastructural controls	343
7.4 Data centre physical access controls	355
7.5 Computer hardware management controls	359
7.6 IT contingency planning and disaster recovery controls	364
7.7 Monitoring and review controls	374
7.8 IT operational performance measures	378

Contents

7.9 Review and audit tools and techniques	380
7.10 Conclusion	393
7.11 Review questions	395
Chapter 8: SYSTEMS SOFTWARE CONTROLS....	399
8.1 Scope	399
8.2 Purpose and main types of systems software controls	400
8.3 Systems software operating environment controls	401
8.4 Database controls	412
8.5 Data communications controls	422
8.6 Audit trail log file controls	434
8.7 Monitoring and review controls	435
8.8 IT technical performance measures	437
8.9 Review and audit tools and techniques	439
8.10 Conclusion	454
8.11 Review questions	455
Chapter 9: IT APPLICATION CONTROLS	459
9.1 Scope	459
9.2 Purpose and main types of IT application controls	460
9.3 Input, processing and output controls	462
9.4 IT application database, operation, change and testing controls	468
9.5 End-user computing controls	481
9.6 Monitoring and review controls	484
9.7 IT application performance measures	485
9.8 Review and audit tools and techniques	486
9.9 Conclusion	509
9.10 Review questions	511
Chapter 10: USING IT CONTROLS IN AUDIT AND CONSULTING ASSIGNMENTS	515
10.1 Scope	515
10.2 Purpose	515
10.3 Retail operation: IT strategy case study	516

10.4 Trading company: applications controls case study	521
10.5 Public organisation: IT security case study	525
10.6 IT audit assignment for organisation 'ABCXYZ'	528
10.7 IT policies and procedures review for company 'ABCXXYX'	554
10.8 Final conclusion	568
APPENDICES: EXAMPLES OF POLICIES, GUIDELINES, FORMS AND METHODOLOGIES.	573
Appendix 1: Examples of IT security policies	573
Appendix 2: Example of IT ethics code	590
Appendix 3: Monitoring IT controls checklist	591
Appendix 4: Examples of IT forms	603
Appendix 5: IT audit methodology	622
Appendix 6: IT audit areas	634
Appendix 7: Internal audit report example	639
FURTHER RESOURCES	641
Books and articles	641
Other resources	656
ITG Resources	659