

Summary Table of Contents

Chapter 1:	Managing Regulatory Compliance Risk
Chapter 2:	Establishing a Data Processing Compliance Function
Chapter 3:	Sample Procedures
Chapter 4:	Sample Checklists
	Part A: Policy Checklists (Available Only on CD)
	Part B: Procedures Checklists (Available Only on CD)
Chapter 5:	Regulatory Data Processing Work Programs
Chapter 6:	Management Reporting
Appendix A:	Bank Service Company Act
Appendix B:	IT-Related Laws and Regulations
Appendix C:	Regulatory Issuances (Issuances Available Only on CD)
Appendix D:	FFIEC IT Examination Handbook (Available Only on CD)
Appendix E:	Glossary

Contents

About the Author.....	iii
How to Use This Manual.....	v
Summary Table of Contents.....	vii

Chapter 1 Managing Regulatory Compliance Risk

Compliance Requirements.....	1 — 1
Identifying Regulatory Risk.....	1 — 2
Management.....	1 — 2
The Planning Process.....	1 — 2
Controls.....	1 — 3
Financial Analysis.....	1 — 3
Systems Development and Programming.....	1 — 4
Documentation.....	1 — 4
Data Integrity.....	1 — 5
Operations.....	1 — 5
Physical Security.....	1 — 6
Additional Risks.....	1 — 6
Analyzing Regulatory Risk.....	1 — 7
Degree of Risk.....	1 — 7
Examination Procedures.....	1 — 8
Quantifying Risk.....	1 — 8
Risk Tolerance Level.....	1 — 8
Managing Regulatory Risk.....	1 — 9
Written Policies and Procedures.....	1 — 9
Other Control Procedures.....	1 — 10
Self-Monitoring.....	1 — 10
Independent Audits.....	1 — 11
Interagency Policy Statement Regarding External Audit.....	1 — 11
Interagency Advisory on the Unsafe and Unsound Use of Limitation of Liability Provisions in External Audit Engagement Letters.....	1 — 12
Limitation of Liability Provisions.....	1 — 13
Auditor Independence.....	1 — 14a
Alternative Dispute Resolution Agreements and Jury Trial Waivers.....	1 — 14b
Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing.....	1 — 14c
FFIEC IT Handbook: Audit Booklet.....	1 — 14c
Corrective Actions.....	1 — 14e
Training.....	1 — 14e
Sarbanes-Oxley Act and Corporate Governance RE: Data Processing.....	1 — 15
Background.....	1 — 15

Insights	1 — 15
Definitions	1 — 16
Specific Review of Sarbanes-Oxley Act	1 — 17
Other Sarbanes-Oxley Act Issues Relevant to Registered Banks	1 — 20
Creation of Public Accounting Board	1 — 21
New Public Accounting Oversight Board	1 — 21
Operations of the Oversight Board	1 — 22
Relationship with FASB	1 — 22
Funding the Public Oversight Board	1 — 23
Applicability of Certain Provisions of the Sarbanes-Oxley Act of 2002 to Institutions That Are Not Public Companies and Are Less Than \$500 Million Total Assets	1 — 23
Title I — Public Company Accounting Oversight Board	1 — 23
Section 102. Registration with the Board	1 — 23
Related Policy Guidance	1 — 23
Title II — Auditor Independence	1 — 24
Section 201. Services Outside the Scope of Practice of Auditors and Section 202. Preapproval Requirements	1 — 24
Related Corporate Governance Guidance RE: Practices for Financial Institutions	1 — 24
Section 203. Audit Partner Rotation	1 — 25
Sound Corporate Governance Practices for Financial Institutions	1 — 25
Section 204. Auditor Reports to Audit Committees	1 — 26
Sound Corporate Governance Practices for Banks	1 — 26
Section 206. Conflicts of Interest	1 — 26
Sound Corporate Governance Practices for Financial Institutions	1 — 26
Title III — Corporate Responsibility	1 — 26
Section 301. Public Company Audit Committees	1 — 26
Related Policy Guidance for Financial Institutions	1 — 27
Sound Corporate Governance Practices for Financial Institutions	1 — 27
Section 302. Corporate Responsibility for Financial Reports	1 — 27
Sound Corporate Governance Practices for Financial Institutions	1 — 27
Section 303. Improper Influence on Conduct of Audits	1 — 28
Sound Corporate Governance Practices for Financial Institutions	1 — 28
Title IV — Enhanced Financial Disclosures	1 — 28
Section 401. Disclosures in Periodic Reports	1 — 28
Sound Corporate Governance Practices for Financial Institutions	1 — 28
Section 402. Enhanced Conflict of Interest Provisions	1 — 28
Related Policy Guidance for Financial Institutions	1 — 29
Section 404. Management Assessment of Internal Controls	1 — 29
Related Policy Guidance for Financial Institutions	1 — 29
Sound Corporate Governance Practices for Financial Institutions	1 — 29
Section 406. Code of Ethics for Senior Financial Officers	1 — 29
Related Policy Guidance for Banks	1 — 30
Sound Corporate Governance Practices for Banks	1 — 30
Section 407. Disclosure of Audit Committee Financial Expert	1 — 30
Sound Corporate Governance Practices for Financial Institutions	1 — 31
Applicability of Certain Provisions of the Sarbanes-Oxley Act of 2002 to Institutions with \$500 Million or More in Total Assets	1 — 31
Auditor Independence	1 — 31
Management’s Responsibility for Financial Reporting and Controls	1 — 33

Management’s Assessment of Internal Controls and Accountant’s Attestation on This Assessment.....	1 — 34
Other Provisions of the Sarbanes-Oxley Act	1 — 34
Cost of Compliance Concerns.....	1 — 35
SOX Effects on Internal Controls and Data Processing (Information Technology (IT)).....	1 — 35
Summary	1 — 37
Risk Assessments and Internal Controls Per ISA 400.....	1 — 38
Background	1 — 38
Control Environment.....	1 — 38
Control Procedures.....	1 — 39
Accounting and Internal Control Systems	1 — 40
Inherent Limitations of Internal Controls	1 — 40
Understanding the Accounting and Internal Control System.....	1 — 40
Control Procedures.....	1 — 41
Control Risk	1 — 41
Preliminary Assessment of Control Risk	1 — 41
SAS 70 Reviews.....	1 — 42
Audit Independence.....	1 — 43
Exhibit 1.1: Internal Audit Review Questionnaire.....	1 — 44
Exhibit 1.2: Auditor Independence Questionnaire.....	1 — 49
Exhibit 1.3: Board/Audit Committee Oversight Questionnaire	1 — 61
Exhibit 1.4: Limitations of Liability Provisions and the SEC’s Auditor Independence Rules	1 — 67

Chapter 2

Establishing a Data Processing Compliance Function

Establishing a Regulatory Compliance Program.....	2 — 1
Who Should Have Review Responsibility?.....	2 — 2
Data Processing Compliance Structure	2 — 3
Data Processing Functional Structure.....	2 — 4
Operations Manager	2 — 4
Systems and Programming Manager.....	2 — 5
Data Base Administrator	2 — 5
Quality Assurance Staff	2 — 5
Data Processing Compliance Committe	2 — 5
Role of the Data Processing Compliance Coordinators	2 — 6
Management Reporting	2 — 6
Additional Large Bank Considerations	2 — 7
Small Bank Considerations	2 — 7
Turnkey Operations.....	2 — 7
Small Systems	2 — 8
Processing Through a Data Center	2 — 8
Types of Services	2 — 8
Control Issues.....	2 — 9
Review of Remote Sites	2 — 10
Exhibit 2.1: IT Remote Site Review Program	2 — 11

Chapter 3 Sample Procedures

Data Processing Compliance Review: Security Policy	3 — 2
Security Policy	3 — 3
Security Procedures	3 — 12
Data Processing Compliance Review: Risk Assessment and Insurance Policy	3 — 25
Risk Assessment and Insurance Policy	3 — 26
Risk Assessment and Insurance Procedures	3 — 28
Data Processing Compliance Review: Data Processing Management Steering Committee Policy	3 — 33
Data Processing Management Steering Committee Policy	3 — 34
Data Processing Management Steering Committee Procedures	3 — 37
Data Processing Compliance Review: Servicing Arrangements Policy	3 — 39
Servicing Arrangements Policy	3 — 40
Servicing Arrangements Procedures	3 — 45
Data Processing Compliance Review: Short- and Long-Range Planning Policy	3 — 51
Short- and Long-Range Planning Policy	3 — 53
Short- and Long-Range Planning Procedures	3 — 56
Data Processing Compliance Review: Electronic Fund Transfer Systems Policy	3 — 60
Electronic Fund Transfer Systems Policy	3 — 62
Electronic Fund Transfer Systems Procedures	3 — 67
Data Processing Compliance Review: Emergency and Disaster Recovery Policy	3 — 75
Emergency and Disaster Recovery Policy	3 — 76
Emergency and Disaster Recovery Procedures	3 — 82
Data Processing Compliance Review: Computer Operations Policy	3 — 93
Computer Operations Policy	3 — 94
Computer Operations Procedures	3 — 100
Data Processing Compliance Review: Software, Programming, and Package Purchase Policy	3 — 105
Software, Programming, and Package Purchase Policy	3 — 106
Data Processing Compliance Review: Microcomputer Policy	3 — 111
Microcomputer Policy	3 — 113
Microcomputer Procedures	3 — 120
Data Processing Compliance Review: Small Bank Data Processing Policy	3 — 128
Small Bank Data Processing Policy	3 — 129
Small Bank Data Processing Procedures	3 — 134
Data Processing Compliance Review: Internal and External EDP Audit Policy	3 — 140
Internal and External EDP Audit Policy	3 — 141
Internal and External EDP Audit Procedures	3 — 147
Data Processing Compliance Review: Accounting for Software Development Costs Policy	3 — 153
Accounting for Software Development Costs Policy	3 — 154
Accounting for Software Development Costs Procedures	3 — 157
Data Processing Compliance Review: Ethics and Employee Conduct for DP Personnel Policy	3 — 159
Ethics and Employee Conduct for DP Personnel Policy	3 — 160
Ethics and Employee Conduct for DP Personnel Procedures	3 — 166
Data Processing Compliance Review: Local Area Networks Policy	3 — 172
Local Area Networks Policy	3 — 173
Local Area Networks Procedures	3 — 178
Data Processing Compliance Review: Data Processing Management Policy	3 — 183

Data Processing Management Policy	3 — 184
Data Processing Management Procedures.....	3 — 187
Data Processing Compliance Review: Contracts with Vendors Policy.....	3 — 191
Contracts with Vendors Policy	3 — 193
Contracts with Vendors Procedures	3 — 199
Data Processing Compliance Review: Electronic Banking Policy.....	3 — 204
Electronic Banking Policy.....	3 — 205
Electronic Banking Procedures	3 — 212
Data Processing Compliance Review: E-Mail Systems Policy.....	3 — 216
E-Mail Systems Policy	3 — 217
E-Mail Systems Procedures.....	3 — 222
Data Processing Compliance Review: Internet Access Policy.....	3 — 225
Internet Access Policy	3 — 226
Internet Access Procedures.....	3 — 233
Data Processing Compliance Review: Online Privacy Policy	3 — 240
Online Privacy Policy.....	3 — 241
Online Privacy Procedures	3 — 246
Data Processing Compliance Review: PC/LAN Management Policy	3 — 250
PC/LAN Management Policy.....	3 — 251
PC/LAN Management Procedures	3 — 254
Data Processing Compliance Review: Outsourcing Policy.....	3 — 256
Outsourcing Policy	3 — 257
Outsourcing Procedures.....	3 — 262
Data Processing Compliance Review: Customer Data Protection/Privacy Policy.....	3 — 265
Customer Data Protection/Privacy Policy	3 — 266
Customer Data Protection/Privacy Procedures.....	3 — 272
Data Processing Compliance Review: Financial Modeling Policy	3 — 276
Financial Modeling Policy	3 — 277
Financial Modeling Procedures	3 — 280
Data Processing Compliance Review: Data Management and Management Information Systems Policy	3 — 282
Data Management and Management Information Systems Policy.....	3 — 284
Data Management and Management Information Systems Procedures	3 — 297
Data Processing Compliance Review: Electronic Banking Information Authentication Policy.....	3 — 320
Electronic Banking Information Authentication Policy	3 — 322
Electronic Banking Information Authentication Procedures.....	3 — 327
Data Processing Compliance Review: Training and Education Policy.....	3 — 335
Training and Education Policy	3 — 336
Training and Education Procedures.....	3 — 342
Data Processing Compliance Review: Regulatory Compliance Risk Management Policy	3 — 348
Regulatory Compliance Risk Management Policy.....	3 — 349
Regulatory Compliance Risk Management Procedures	3 — 356
Data Processing Compliance Review: Forms Management Policy	3 — 360
Forms Management Policy.....	3 — 361
Forms Management Procedures	3 — 367
Data Processing Compliance Review: Electronic Imaging Policy.....	3 — 372
Electronic Imaging Policy	3 — 373
Electronic Imaging Procedures.....	3 — 378
Data Processing Compliance Review: Service Requests Policy	3 — 382

Service Requests Policy	3 — 383
Service Requests Procedures	3 — 389
Data Processing Compliance Review: Personal Computer End User Security Policy.....	3 — 395
Personal Computer End User Security Policy	3 — 397
Data Processing Compliance Review: Microcomputer Controls Policy	3 — 402
Microcomputer Controls Policy	3 — 403
Microcomputer Controls Procedures.....	3 — 408
Data Processing Compliance Review: Transaction Processing Policy	3 — 413
Transaction Processing Policy.....	3 — 414
Transaction Processing Procedures	3 — 419
Data Processing Compliance Review: Information Security Policy	3 — 424
Information Security Policy	3 — 426
Information Security Procedures.....	3 — 436
Data Processing Compliance Review: Terrorism Incident Response Policy	3 — 457
Terrorism Incident Response Policy.....	3 — 459
Terrorism Incident Response Procedures	3 — 463
Data Processing Compliance Review: Server Security Policy	3 — 467
Server Security Policy	3 — 469
Server Security Procedures.....	3 — 475
Data Processing Compliance Review: Data and Records Destruction Policy.....	3 — 481
Data and Records Destruction Policy.....	3 — 482
Data and Records Destruction Procedures	3 — 488
Data Processing Compliance Review Procedures: Forms Design Policy	3 — 494
Forms Design Procedures.....	3 — 500
Data Processing Compliance Review: Controls Review Policy.....	3 — 506
Controls Review Policy.....	3 — 508
Data Processing Compliance Review: Incident Response Policy	3 — 512
Incident Response Procedures	3 — 514
Data Processing Compliance Review: Outsourcing Information Security Policy	3 — 536
Outsourcing Information Security Procedures	3 — 540
Data Processing Compliance Review Procedures: Automated Clearing House Policy	3 — 566
Automated Clearing House Policy	3 — 568
Data Processing Compliance Review Procedures: Vendor Management Policy	3 — 579
Vendor Management Policy	3 — 580
Data Processing Compliance Review Procedures: Vendor Management Procedures	3 — 586
Vendor Management Procedures	3 — 587
Data Processing Compliance Review: Remote Deposit Capture Policy	3 — 593
Remote Deposit Capture Policy	3 — 595
Remote Deposit Capture Procedures.....	3 — 609

Chapter 4
Sample Checklists
(Available Only on CD)

Part A
Policy Checklists

Security.....	4A — 1
Risk Assessment and Insurance.....	4A — 58
Data Processing Management Steering Committee	4A — 68
Servicing Arrangements	4A — 73
Short- and Long-Range Planning	4A — 82
Electronic Fund Transfer Systems.....	4A — 87
Emergency and Disaster Recovery.....	4A — 94
Computer Operations.....	4A — 105
Software, Programming, and Package Purchase	4A — 116
Microcomputer	4A — 124
Small Bank Data Processing	4A — 135
Internal and External EDP Audit.....	4A — 143
Accounting for Software Development Costs	4A — 154
Ethics and Employee Conduct for DP Personnel	4A — 160
Local Area Networks.....	4A — 170
Data Processing Management	4A — 179
Contracts with Vendors	4A — 183
Electronic Banking.....	4A — 193
E-Mail Systems	4A — 207
Internet Access	4A — 215
Online Privacy	4A — 225
PC/LAN Management.....	4A — 233
Outsourcing	4A — 238
Customer Data Protection/Privacy	4A — 245
Financial Modeling.....	4A — 255
Data Management and Management Information Systems.....	4A — 260
Electronic Banking Information Authentication	4A — 277
Training and Education	4A — 285
Regulatory Compliance Risk Management.....	4A — 293
Forms Management.....	4A — 304
Electronic Imaging	4A — 313
Service Requests.....	4A — 320
Personal Computer End User Security	4A — 330
Microcomputer Controls	4A — 338
Transaction Processing.....	4A — 346
Personal Computer Security	4A — 354
Information Security.....	4A — 360
Terrorism Incident Response.....	4A — 375
Server Security	4A — 381

Data and Records Destruction	4A — 390
Forms Design	4A — 399
Vendor Management	4A — 409
Contracting for External Data Processing Services.....	4A — 415
Incident Response.....	4A — 429
Automated Clearing House	4A — 442
Remote Deposit Capture.....	4A — 462

Part B Procedures Checklists

Security.....	4B — 1
Risk Assessment and Insurance.....	4B — 19
Data Processing Management Steering Committee	4B — 28
Servicing Arrangements	4B — 32
Short- and Long-Range Planning	4B — 44
Electronic Fund Transfer Systems.....	4B — 51
Emergency and Disaster Recovery.....	4B — 68
Computer Operations.....	4B — 112
Software, Programming, and Package Purchase	4B — 123
Microcomputer	4B — 136
Internal and External EDP Audit.....	4B — 166
Accounting for Software Development Costs	4B — 179
Ethics and Employee Conduct for DP Personnel	4B — 182
Local Area Network	4B — 195
Data Processing Management	4B — 206
Contracts with Vendors	4B — 213
Electronic Banking	4B — 224
E-Mail Systems	4B — 230
Internet Access	4B — 236
Online Privacy	4B — 253
PC/LAN Management	4B — 260
Outsourcing	4B — 263
Customer Data Protection/Privacy	4B — 268
Financial Modeling.....	4B — 275
Data Management and Management Information Systems.....	4B — 279
Electronic Banking Information Authentication	4B — 315
Data Processing Training and Education.....	4B — 332
Forms Management	4B — 341
Service Request	4B — 352
Data Processing Forms Management	4B — 363
Personal Computer End User Security	4B — 373
Microcomputer Controls	4B — 381
Transaction Processing	4B — 390
Electronic Imaging	4B — 400
Terrorism Incident Response.....	4B — 407
Server Security	4B — 416

Information Security.....	4B — 429
Data and Records Destruction.....	4B — 475
Forms Design.....	4B — 481
Vendor Management.....	4B — 491
Contracting for External Data Processing Services.....	4B — 497
Controls Review.....	4B — 512
Incident Response Procedures Checklist.....	4B — 547
Vendor Management.....	4B — 561
Outsourcing Information.....	4B — 567

Chapter 5 Regulatory Data Processing Work Programs

Examination Procedures.....	5 — 1
Using the Work Programs.....	5 — 2

Chapter 6 Management Reporting

Presenting the Information.....	6 — 1
Format.....	6 — 1
Efficient Communication.....	6 — 2
Exhibit 6.1: Data Processing Compliance Committee.....	6 — 3
Exhibit 6.2: Board of Directors Audit and Compliance Committee Reporting Agenda.....	6 — 4
Exhibit 6.3: Data Processing Compliance Committee Follow-Up Format Sheet.....	6 — 5
Exhibit 6.4: Regulatory Data Processing Compliance Reviews.....	6 — 6
Exhibit 6.5: Data Processing Department Corrective Action Plan Status Report.....	6 — 8
Exhibit 6.5: Data Processing Department Corrective Action Plan Status Report.....	6 — 8

Appendix A
Bank Service Company Act

Appendix B
IT-Related Laws and Regulations

Appendix C
Regulatory Issuances
(Issuances Available Only on CD)

Appendix D
FFIEC IT Examination Handbook
(Available Only on CD)

Appendix E
Glossary