

CONTENTS

| | | |
|---------------------|--|----------|
| Introduction | | 1 |
| | Part 1: The Fundamentals | 3 |
| Chapter | | |
| 1 | PCI Fundamentals | 5 |
| | History of PCI | 7 |
| | Why PCI DSS? | 8 |
| Chapter | | |
| 2 | Security 101 | 19 |
| | Strategy and Planning | 20 |
| | Information Risk Management | 20 |
| | Information Classification | 23 |
| | Risk Assessment | 24 |
| | Risk Analysis | 26 |
| | Dealing With Risk | 27 |
| | Defense in Depth | 28 |
| | Policy, Standards, and Procedures | 28 |
| | Adoption of a Security Framework | 31 |
| | Security and the System Development Life Cycle (SDLC) | 35 |
| | Security Training and Awareness | 37 |
| | Metrics | 39 |
| | Physical Security | 40 |
| | Data Communications and Networking | 42 |
| | Perimeter Security | 43 |

| | | |
|----------------|---|-----------|
| | Information Security Monitoring and Log Management | 44 |
| | Intrusion Detection and Intrusion Prevention Technology | 46 |
| | Logical Access Control | 48 |
| | Electronic Authentication | 49 |
| | Encryption | 50 |
| | Remote Access Control | 53 |
| | Secure Communications | 53 |
| | HTTPS | 53 |
| | Secure Shell | 54 |
| | Virtual Private Networks | 54 |
| | Wireless | 55 |
| | Incident Response | 57 |
| | Forensics | 58 |
| | Part 2: PCI Breakdown (Control Objectives and Associated Standards) | 61 |
| Chapter | | |
| 3 | Build and Maintain a Secure Network | 63 |
| | Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data | 63 |
| | Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters | 76 |
| | Requirement A.1: Hosting Providers Protect Cardholder Data Environment | 81 |
| Chapter | | |
| 4 | Protect Cardholder Data | 83 |
| | Requirement 3: Protect Stored Cardholder Data | 83 |
| | PCI DSS Appendix B: Compensating Controls for Requirement 3.4 | 90 |
| | Requirement 4: Encrypt Transmission of Cardholder Data Across Open Public Networks | 96 |

| | | |
|----------------|---|------------|
| Chapter | | |
| 5 | Maintain a Vulnerability Management Program | 99 |
| | Requirement 5: Use and Regularly Update Antivirus Software | 99 |
| | Requirement 6: Develop and Maintain Secure Systems and Applications | 101 |
| Chapter | | |
| 6 | Implement Strong Access Control Measures | 123 |
| | Requirement 7: Restrict Access to Cardholder Data by Business Need to Know | 124 |
| | Requirement 8: Assign a Unique ID to Each Person with Computer Access | 124 |
| | Requirement 9: Restrict Physical Access to Cardholder Data | 131 |
| Chapter | | |
| 7 | Regularly Monitor and Test Networks | 141 |
| | Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data | 142 |
| | Requirement 11: Regularly Test Security Systems and Processes | 148 |
| Chapter | | |
| 8 | Maintain an Information Security Policy | 155 |
| | Requirement 12: Maintain a Policy that Addresses Information Security | 156 |
| | Part 3: Strategy and Operations | 173 |
| Chapter | | |
| 9 | Assessment and Remediation | 175 |
| | PCI DSS Payment Card Industry Self-Assessment Questionnaire | 175 |
| | PCI DSS Security Audit Procedures | 176 |
| | PCI DSS Security Scanning Procedures | 176 |
| | Leveraging Self-Assessment | 176 |
| | Strategy and Program Development | 177 |

Chapter

| | | |
|-----------|---|------------|
| 10 | PCI Program Management | 179 |
| | Case for Strategic Compliance | 180 |
| | Who Should Be Involved Achieving | |
| | PCI DSS Compliance for Our Organization? | 182 |
| | <i>PCI DSS Glossary, Abbreviations, and Acronyms</i> | 185 |
| | <i>References</i> | 201 |
| | <i>Resources</i> | 203 |
| | <i>Index</i> | 209 |

<http://www.pbookshop.com>