Risk Management in Electronic Banking: Concepts and Best Practices

Jayaram Kondabagil

John Wiley & Sons (Asia) Pte Ltd.
PART I: INTRODUCTION TO E-BANKING

Chapter 1  E-Banking Basics 3
Evolution of e-banking 3
Impact on traditional banking 4
E-banking components 7
Regulatory approval 8

Chapter 2  E-Banking Risks 10
Strategic risk 11
Operational risk 12
Compliance risk 13
Reputational risk 13
## Contents

| Other risks | 14 |
| Risk management challenges | 15 |
| The five-pillar approach | 17 |

**Chapter 3** Product and Service-specific Risks 19

- Internet banking 19
- Aggregation services 21
- Bill presentment and payment 23
- Mobile banking 24
- Weblinking 25
- Electronic money 27
- Cross-border transactions 27
- New products and services 29

**PART II: RISK MANAGEMENT**

**Chapter 4** Risk Management Framework 33

- Policies and procedures 34
- Risk management process 35
- Operational risk management 39
- Governance and internal controls 40

**Chapter 5** Risk Management Organization 43

- Organization structure 43
- Board and senior management 44
- Executive risk committee 49
- IT management 51
- Internal and external audit 53

**Chapter 6** International Standards 56

- Basel Committee on banking supervision 56
- COBIT 4.0 57
- ISO 17799 58
- OCTAVE 59
- COSO – enterprise risk management 60
- PCI data security standard 61
- Financial Action Task Force 62
Corporate governance codes 63
Regulatory guidelines 64

Part III: INFORMATION SECURITY

Chapter 7 Information Security Management 69
Security objectives 70
Security controls 73
Security risk assessment 76
Classification of controls 78
Monitoring and testing 79
Incident response plan 80

Chapter 8 Operational Controls 82
Personnel issues 82
Segregation of duties 84
Technical issues 86
Database management 88
Change management 89
Backups and off-site storage 90
Insurance 92
Fraud management 93

Chapter 9 Technical Controls 97
Logical access controls 98
Identification and authentication 99
Authentication methods 101
Audit trails 104
Network security 105
Firewalls 108
Malicious code 110
Information security incidents 111

PART IV: OUTSOURCING

Chapter 10 Outsourcing in E-Banking 117
Types of outsourcing 118
Material outsourcing 119
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisory approach</td>
</tr>
<tr>
<td>Key risks of outsourcing</td>
</tr>
<tr>
<td>Board and senior management responsibility</td>
</tr>
<tr>
<td>Outsourcing policy</td>
</tr>
</tbody>
</table>

Chapter 11 Managing Outsourced Services 126
- Outsourcing decisions | 126
- Risk assessment and control | 127
- Service provider due diligence | 130
- Offshoring | 131
- Contingency plans | 132
- Customer service | 132
- Monitoring and audit | 134

Chapter 12 Outsourcing Contracts 137
- Contractual provisions | 138
- Right of access clauses | 140
- Termination clause | 141
- Offshoring contracts | 141
- Confidentiality and security clauses | 142
- Business continuity clauses | 144

PART V: BUSINESS CONTINUITY

Chapter 13 Business Continuity Management 147
- The main drivers | 147
- Board and senior management responsibility | 149
- Components of BCM | 151
- Business impact analysis | 152
- BIA methodologies | 153
- Recovery strategy | 156

Chapter 14 Business Continuity Plan 158
- Major components of BCP | 158
- Continuity management team | 160
- Recovery procedures | 162
- Resource requirements | 163
- External communications | 165
Plan maintenance 167
Awareness and training 169
Testing of BCP 171
Testing methods 172

Chapter 15 Data Centers and Alternate Sites 175
Evolution of data centers 175
Location of the sites 176
Mitigating concentration risk 177
Data center design 178
Logistics management 180
Maintenance procedures 182
Alternate site models 183
External support 185
Business continuity in real life 186

PART VI: LEGAL AND REGULATORY COMPLIANCE 193

Chapter 16 Compliance Function 194
Organization of the compliance function 194
Board and senior management responsibility 195
Role of regulators 196

Chapter 17 Major Compliance Issues 198
Anti-money laundering 198
Know your customer (KYC) 199
Suspicious activities 201
Privacy of customer information 202
Information disclosures 204
Customer education 206

High-level review checklist 209
Acronyms 225
Glossary 227
References 245
Index 251