



RISK MANAGEMENT & RISK ASSESSMENT PROGRAM

- HIPAA/HEALTHCARE - PREMIER EDITION

Insert Company Logo

TABLE OF CONTENTS

Overview	1
Key Terms	1
Vulnerability	
Threat	
Risk	
Risk Summary	
Risk Likelihood	
Risk Impact Rating	
Overall Risk Rating	
Categories of Risk	
Information Security Risks and Vulnerabilities Topics	7
Senior Management	
Asset Inventory	
Defense-in-Depth	
Layered Security	
Network Architecture and Configuration	
Network Topology	
Network Security	
Data and Information Classification	
Physical and Environmental Security	
Personnel (Disciplinary Action, Criminal Action, Terminations, Security Awareness Training)	
Provisioning and Hardening	
Time Synchronization	
Access Rights	
Two-Factor Authentication	
Remote Access	
Malware	
Configuration Management	
Vulnerability Management	
Change Control/Change Management	
Software Development Life Cycle	
Information Technology Quality Assurance	
Security and Patch Management	
Backups	
Encryption	
Event Monitoring	
Configuration and Change Monitoring	

Insert Company Logo

Performance and Utilization Monitoring
Logging and Reporting
Incident Response
Vulnerability Scanning
Penetration Testing
BCDRP/CP
Third-Party Vendor Management
Server Virtualization
Cloud Computing

PII & PHI Risks and Vulnerabilities Topics 33

- 164.308 (a)(1)(i): PII & PHI Initiatives
- 164.308 (a)(1)(ii)(A) – 164.308 (a)(1)(ii)(B): PII & PHI Risk Analysis
- 164.308 (a)(1)(ii)(C): Workforce Sanctions
- 164.308 (a)(1)(ii)(D): Regular Review of Information System Activity Review
- 164.308 (a)(2): Security Official
- 164.308 (a)(3)(i): Workforce Security
- 164.308 (a)(3)(ii)(A): Authorization and/or Supervision
- 164.308 (a)(3)(ii)(B): Workforce Clearance Procedures
- 164.308 (a)(3)(ii)(C): Termination Procedures
- 164.308 (a)(4)(i): Information Access Management
- 164.308 (a)(4)(ii)(A): Isolating Health Care Clearinghouse Functions
- 164.308 (a)(4)(ii)(B): Access Authorization
- 164.308 (a)(4)(ii)(C): Access Establishment and Modification
- 164.308 (a)(5)(i): Security Awareness and Training
- 164.308 (a)(5)(ii)(A): Security Reminders
- 164.308 (a)(5)(ii)(B): Protection from Malicious Software
- 164.308 (a)(5)(ii)(C): Log-in Monitoring
- 164.308 (a)(5)(ii)(D): Password Management
- 164.308 (a)(6)(i): Security Incident Procedures
- 164.308 (a)(6)(ii): Response and Reporting
- 164.308 (a)(7)(i): Contingency Plan
- 164.308 (a)(7)(ii)(A): Data Backup Plan
- 164.308 (a)(7)(ii)(B): Disaster Recovery Plan
- 164.308 (a)(7)(ii)(C): Emergency Mode Operation Plan
- 164.308 (a)(7)(ii)(D): Testing and Revision Procedures
- 164.308 (a)(7)(ii)(E): Application and Data Criticality Analysis
- 164.308 (a)(8): Evaluation
- 164.308 (b)(1) – 164.308 (b)(3): Business Associate Contracts
- 164.310 (a)(1): Facility Access Controls
- 164.310 (a)(2)(i): Contingency Operations
- 164.310 (a)(2)(ii): Facility Security Plan

Insert Company Logo

- 164.310 (a)(2)(iii): Access Control and Validation Procedures
- 164.310 (a)(2)(iv): Maintenance Records
- 164.310 (b): Workstation Use
- 164.310 (c): Workstation Security
- 164.310 (d)(1): Device and Media Controls
- 164.310 (d)(2)(i): Disposal
- 164.310 (d)(2)(ii): Media Re-use
- 164.310 (d)(2)(iii): Accountability
- 164.310 (d)(2)(iv): Data Backup and Storage
- 164.312 (a)(1): Access Control
- 164.312 (a)(2)(i): Unique User Identification
- 164.312 (a)(2)(ii): Emergency Access Procedure
- 164.312 (a)(2)(iii): Automatic Logoff
- 164.312 (a)(2)(iv): Encryption and Decryption
- 164.312 (b): Audit Controls
- 164.312 (c)(1): Integrity
- 164.312 (c)(2): Mechanisms to Authenticate Electronic Protected Health Information
- 164.312 (d): Person or Entity Authentication
- 164.312 (e)(1): Transmission Security
- 164.312 (2)(i): Integrity Controls
- 164.312 (e)(2)(ii): Encryption
- 164.316 (a): Policies and Procedures
- Additional Requirements: Policies and Procedures I
- Additional Requirements: Policies and Procedures II
- Additional Requirements: Breach Notification

Cardholder Data Risks and Vulnerabilities Topics 50

- Firewalls
- Vendor Supplied Defaults
- Protection of Cardholder Data
- Encrypting Transmission of Cardholder Data
- Malware
- Developing and Maintaining Secure Applications
- Restricting Access to Cardholder Data
- Identifying and Authenticating Access to Cardholder Data
- Physical Access to Cardholder Data
- Tracking and Monitoring Access
- Testing Security Systems
- Policies and Procedures for Addressing Information Security

Compliance Risks and Vulnerabilities Topics	53
Record of Compliance	
Compliance Management System	
Clear Commitment to Compliance	
Authority and Accountability for Compliance Risks	
Management Participation and Responding to Changes	
Compliance Considerations	
Controls and Systems for Identifying Compliance Problems	
Training Programs for Compliance	
Management’s Ability to Understand Compliance	
Reputation Risks and Vulnerabilities Topics	56
Management and Board Oversight	
Assessing and Implementing Risk Measures	
Communicating, Educating, Reaching Out, “Brand Building”	
Monitoring the Organization’s “Brand” and “Identity”	
Corporate Values	
“Quality”	
Interaction with Stakeholders	
System of Internal Controls	
Measures for Responding to Incidents	
Strategic Risks and Vulnerabilities Topics	59
Clearly Defined Objectives and Vision	
Leadership from Executive Officers	
Constant Communication	
Proper Resource Allocation	
Response Mechanisms to Changes	
Operational Risks and Vulnerabilities Topics	61
Risk Planning	
Business Continuity and Disaster Recovery (BCDRP) Planning	
Asset Control and Record Keeping	
Supervision and Oversight	
Senior Management Skill Sets and Knowledge	
Training, Cross-Training, and Knowledge Building	
Workflow Documentation	
Adequate Segregation of Duties	
Reconciliation and Auditing of Organizational Assets	
Critical Legal Issues	
Organizational Planning and Response	

Transaction Risks and Vulnerabilities Topics	64
Anticipating and Responding to Risks	
Implementing Sound Operational Processes	
Identifying Weaknesses in Transaction Processing	
Appropriate Monitoring of Transaction Volumes	
Continuity and Reliability of Services	
Managing and Protecting Data	
Risks from New Products and Services	
Understanding of Technology Risks	
Credit Risks and Vulnerabilities Topics	67
Sound Credit Responsibilities re: Apply for Credit.	
Sound Credit Responsibilities re: Offer Credit.	
Credit Knowledge and Expertise	
Payments for Credits Received are Paid Regularly	
Credit Granted to Recipients are Collected Regularly	
Country Risks and Vulnerabilities Topics	69
Assessment of Attitude of Consumers in Host Country	
Assessment of Attitude of Host Country	
Assessment of Currency Inconvertibility	
Assessment of Blockage of Fund Transfers	
Assessment of War, Bureaucracy, and Corruption	
Assessment of Current and Potential State of Country's Economy	
Assessment of Indicators of Economic Growth, Decline, Flat Line, etc.	
Assessment of the Physical Security of Products and Goods	
Assessment of the Physical Security of Employees and Personnel	
Third-Party Risks and Vulnerabilities Topics	72
Documented Due-Diligence Measures for Choosing Vendors	
Measures for Assessing and Evaluating Current Vendors	
Review and Approval of all Contractual Documentation with Vendors	
Management Oversight and Continuous Monitoring of Vendors	
Interest Rate Risks and Vulnerabilities Topics	74
Awareness of Responsibilities by the Board and Senior Management	
Understanding of the Nature and Level of Interest Rate Risk	
Measures Designed to Control Nature and Amount of Interest Rate Risk	
Approval of Business Strategies Governing Interest Rate Risk	

Insert Company Logo

Review and Approval of Measures Identifying Lines of Responsibility that Govern Interest Rate Risk
Discussions and Meetings Amongst Senior Management, Board, etc., regarding Interest Rate Risk
Measures for Managing Interest Rate Risk
Measures and Operating Standards for Interest Rate Risk
Management Activities Related to Interest Rate Risk are Conducted by Competent Staff
Articulation of Overall Objectives and Guidance Regarding Interest Rate Risk

Liquidity Risks and Vulnerabilities Topics78

Clearly Defined Liquidity Strategy
Evaluation of Liquidity Strategy on a Regular Basis
Liquidity Strategy as a Whole
Board and Management Roles
Liquidity Risk Management Structure
Review and Approval of Liquidity Specific Policies and Procedures
Assessment of Cash Inflows and Outflows
Assessment of Short-Term and Long-Term Liquidity Needs
Regular Review of Funding Strategies
Measures for Ensuring Liquid Assets can be Used
Diversification Regarding Liquidity
Efforts to Establish and Maintain Relationships with Liability Holders
Adoption and Implementation of Contingency Funding Plans
Strategy for Addressing Liquidity Shortfalls

Legal Risks and Vulnerabilities Topics82

Existence and Location of Key Organizational Documents
Existence and Location of Additional Key Organizational Documents
Annual Review of Key Organizational Documents
Annual Review of Additional Key Organizational Documents
Annual Review of all Relevant Customer/Client Contracts
Annual Review of all Relevant Human Resources and Organizational Documents
Annual Review of all Critical Financial and Tax Matters
Handling of all Current Legal Issues, etc.
Handling of all Fiscal Management Issues, etc.
Annual Review of all Relevant Intellectual Property Matters, etc.
Legal Exposure to the Organization from any Third-Party Entities

Market Risks and Vulnerabilities Topics86

Development of Broad Based Measures Relating to Market Risk Management
Development of Internal Rules and Organizational Frameworks
Development of Internal Audit Guidelines

Insert Company Logo

Appendix	88
Risk Management & Risk Assessment Policy and Procedures Template	
Terms of Use and Licensing	101