FDIC	Information Technology Examination Officer's Questionnaire

Instructions for Completing the Information Technology Examination Officer's Questionnaire

Please answer the following information security program questions as of the examination date pre-determined by the FDIC. The majority of the questions require only a "Yes" or "No" response; however, you are encouraged to expand or clarify any response as needed directly below each question, or at the end of this document under the heading "Clarifying or Additional Comments". For any question deemed non-applicable to your institution or if the answer is "None", please respond accordingly ("NA" or "None"). Please do not leave responses blank. At the bottom of this document is a signature block, which must be signed by an executive officer attesting to the accuracy and completeness of all provided information.

I hereby certify that the following statements are true and correct to the best of my knowledge and belief.		
Officer's Name and Title	**Institution's Name and Location**	
Officer's Signature	**Date Signed**	**As of Date**
This is an official document. Any false information contained in it may be grounds for prosecution and may be punishable by fine or imprisonment.		

PART 1 – RISK ASSESSMENT

An IT risk assessment is a multi-step process of identifying and quantifying threats to information assets in an effort to determine cost effective risk management solutions. To help us assess your risk management practices and the actions taken as a result of your risk assessment, please answer the following questions:

a. Name and title of individual(s) responsible for managing the IT risk assessment process:

b. Names and titles of individuals, committees, departments or others participating in the risk assessment process. If third-party assistance was utilized during this process, please provide the name and address of the firm providing the assistance and a brief description of the services provided:

c. Completion date of your most recent risk assessment:

d. Is your risk assessment process governed by a formal framework/policy (Y/N)?

e. Does the scope of your risk assessment include an analysis of internal and external threats to confidential customer and consumer information as described in Part 364, Appendix B, of the FDIC’s Rules and Regulations (Y/N)?

f. Do you have procedures for maintaining asset inventories (Y/N)?

g. Do risk assessment findings clearly identify the assets requiring risk reduction strategies (Y/N)?

h. Do written information security policies and procedures reflect risk reduction strategies identified in “g” above (Y/N)?

i. Is your risk assessment *program* formally approved by the Board of Directors at least annually (Y/N)?

   If yes, please provide the date that the risk assessment program was last approved by the Board of Directors:

j. Are risk assessment *findings* presented to the Board of Directors for review and acceptance (Y/N)?

   If yes, please provide the date that the risk assessment findings were last approved by the Board of Directors:

PART 2 – OPERATIONS SECURITY AND RISK MANAGEMENT

To help us assess how you manage risk through your information security program, please answer the following questions for your environment. If any of the following questions are not applicable to your environment, simply answer “N/A.”

a. Please provide the name and title of your formally designated IT security officer:

b. Please provide the name and title of personnel in charge of operations:

c. Do you maintain topologies, diagrams, or schematics depicting your physical and logical operating environment(s) (Y/N)?

d. Does your information security program contain written policies, procedures, and guidelines for securing, maintaining, and monitoring the following systems or platforms:

1. Core banking system (Y/N)?
2. Imaging (Y/N)?
3. Fed Line and/or wire transfer (Y/N)?
4. Local area networking (Y/N)?
5. Wide-area networking (Y/N)?
6. Wireless networking – LAN or WAN (Y/N)?
7. Virtual private networking (Y/N)?
8. Voice over IP telephony (Y/N)?
9. Instant messaging (Y/N)?
10. Portable devices such as PDAs, laptops, cell phones, etc. (Y/N)?
11. Routers (Y/N)?
12. Modems or modem pools (Y/N)?
13. Security devices such as firewall(s) and proxy devices. (Y/N)?
14. Other remote access connectivity such as GoToMyPC, PcAnyWhere, etc. (Y/N)?
15. Other – please list:

e. Do you have formal logging/monitoring requirements for 1-15 above (Y/N)?

f. Do you have formal configuration, change management, and patch management procedures for all applicable platforms identified in “d.” above (Y/N)?

g. Do you have an antivirus management program to protect systems from malicious content (Y/N)?

h. Do you have an anti-spyware management program to protect end-user systems (Y/N)?

i. Do you have a formal intrusion detection program, other than basic logging, for monitoring host and/or network activity (Y/N)?

j. Has vulnerability testing been performed on internal systems (Y/N)?

If yes, please provide date performed and by whom:

k. Has penetration testing of your public or Internet-facing connection(s) been performed (Y/N)?

If yes, please provide date performed and by whom:

l. Do you have an incident response plan defining responsibilities and duties for containing damage and minimizing risks to the institution (Y/N)?

If yes, does the plan include customer notification procedures (Y/N)?

m. Do you have a physical security program defining and restricting access to information assets (Y/N)?

n. Do you have a vendor management program (Y/N)?

o. Are all of your service providers located within the United States (Y/N)?

p. Do you have an employee acceptable use policy (Y/N)?

If yes, please provide how often employees must attest to the policy contents:

q. Do you have an employee security awareness training program (Y/N)?

If yes, please indicate the last date training was provided:

r. Are you planning to deploy new technology within the next 12 months (Y/N)?

If you answered “Yes”, were the risks associated with this new technology reviewed during your most recent risk assessment (Y/N)?

s. Have you deployed new technology since the last FDIC examination that was not included in your last risk assessment (Y/N)?

t. Is security incorporated into your overall strategic planning process (Y/N)?

u. Do you have policies/procedures for the proper disposal of information assets (Y/N)?

PART 3 – AUDIT/INDEPENDENT REVIEW PROGRAM

To help us assess how you monitor operations and compliance with your written information security program, please answer the following questions:

a. Please provide the name and title of your IT auditor or employee performing internal IT audit functions. Include who this person reports to, and a brief description of their education and experience conducting IT audits.

b. Do you have a written IT audit/independent review program (Y/N)?

c. Please provide the following information regarding your most recent IT audit/independent review:

1. Audit Date:
2. Firm name (if external):
3. Was an audit report produced (Y/N)?
4. Date audit report was reviewed and approved by the Board:
5. Audit scope and objectives:

d. Does audit coverage include a comparison of actual system configurations to documented/baseline configuration standards (Y/N)?

e. Does audit coverage include assessing compliance with the information security program requirements (Y/N)?

f. Does audit coverage include assessing users and system services access rights (Y/N)?

g Is audit involved in your risk assessment process (Y/N)?

h. Briefly describe any security incidents (internal or external) affecting the bank or bank customers occurring since the last FDIC IT examination.

i. Briefly describe any known conflicts or concentrations of duties.

PART 4 - DISASTER RECOVERY AND BUSINESS CONTINUITY

To help us assess your preparedness for responding to and recovering from an unexpected event, please answer the following:

a. Do you have an organization-wide disaster recovery and business continuity program (Y/N)?

If yes, please provide the name of your coordinator:

b. Are disaster recovery and business continuity plans based upon a business impact analyses (Y/N)?

If yes, do the plans identify recovery and processing priorities (Y/N)?

c. Is disaster recovery and business continuity included in your risk assessment (Y/N)?

d. Do you have formal agreements for an alternate processing site and equipment should the need arise to relocate operations (Y/N)?

e. Do business continuity plans address procedures and priorities for returning to permanent and normal operations (Y/N)?

f. Do you maintain offsite backups of critical information (Y/N)?

If “Yes,” is the process formally documented and audited (Y/N)?

g. Do you have procedures for testing backup media at an offsite location (Y/N)?

h. Have disaster recovery/business continuity plans been tested (Y/N)?

If “Yes”, please identify the system(s) tested, the corresponding test date, and the date reported to the Board:

PART 5 – Gramm-Leach-Bliley Act/FDIC Rules and Regulations – 12 CFR Part 364 Appendix B

The Interagency Guidelines Establishing Information Security Standards require each bank to have a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. Please answer the following questions pertaining to your written information security program:

a. Has management developed a written information security program meeting the information security standards of Part 364, Appendix B (Y/N)?

If you answered “Yes” to question “a” above, please provide the date that the Board of Directors last approved the written information security program:

b. Please provide the names and titles and/or committee members charged with formally overseeing and implementing Part 364, Appendix B, requirements:

c. Are compliance audits of your Part 364 standards periodically performed and formally reported to the Board of Directors (Y/N)?

If you answered “Yes” to question “c”, please provide the date of your last Part 364 compliance audit or review:

d. Have employees received Part 364 related security awareness training (Y/N)?

e. Please describe the bank’s reporting process for communicating Part 364 program and compliance status to the Board of Directors:

Clarifying or Additional Comments