Information Technology Officer's Questionnaire

Instructions for Completing the Information Technology Officer's Questionnaire

The Information Technology Officer's Questionnaire (Questionnaire) contains questions covering significant areas of a bank's information technology (IT) function. Your responses to these questions will help determine the scope of the examination; provide insight into the composition of the bank's IT operations, information security program, and IT governance processes; and may be relied upon to form conclusions as to the condition of the bank's IT functions. Therefore, accurate and timely completion of the Questionnaire is expected. Examiners may request additional supporting documentation to assess the validity of the answers that are provided and to further assess the quality and content of the bank's IT operations and information security and IT governance programs.

Please answer the 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 near 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 blank responses.

Many questions contain a reference to regulations, guidelines, or supervisory guidance. Additionally, a chart entitled "Interagency Guidelines Establishing Information Security Standards" has been included at the end of this document. The referenced regulations, guidelines, guidance and the attached chart are tools that may aid you in completing the Questionnaire. Please note that these references may not encompass the entirety of published information. Financial institutions are strongly encouraged to be familiar with all applicable laws and regulations, financial institution letters (FILs), and guidance in the FFIEC IT Examination Handbooks.

At the bottom of this page 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:
[*FDIC Rules and Regulations Part 364 Appendix B Section III (A)(2)*]

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:
[*FDIC Rules and Regulations Part 364 Appendix B Section III (A)(2)*]

c. Does your written information security program include a risk assessment (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (B)*]

d. Does the scope of your risk assessment include an enterprise-wide analysis of internal and external threats and vulnerabilities to confidential customer and consumer information; the likelihood and impact of identified threats and vulnerabilities; and the sufficiency of policies, procedures, and customer information systems to control risks (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (B)*]

e. Do you have procedures for maintaining asset inventories and identifying customer information at the bank, in transit, and at service providers (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (B); FFIEC IT Examination Handbook, Information Security Booklet*]

f. Do risk assessment findings clearly identify the assets requiring risk reduction strategies (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (B); FFIEC IT Examination Handbook, Information Security Booklet*]

g. Do written information security policies and procedures reflect risk reduction strategies for the assets identified in "f" above (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1); FFIEC IT Examination Handbook, Information Security Booklet*]

h. Were changes in technology (e.g. service provider relationships, software applications, and/or service offerings) implemented since the previous FDIC examination reflected in your risk assessment (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C),(E); FFIEC IT Examination Handbook, Information Security Booklet*]

If "No," what technology changes were excluded?

i. Is your risk assessment *program* formally approved by the Board of Directors at least annually (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (A)(1) and (F)*]

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

j. Has a report of risk assessment *findings* been presented to the Board of Directors for review and acceptance (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (F)*]

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

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

If "Yes," were the risks associated with this new technology reviewed during your most recent risk assessment (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (E); FFIEC IT Examination Handbook, Information Security Booklet*]

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. Do you have a written information security program designed to manage and control risk (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section II (A) and Section III (C)(1)*]

If "Yes," please provide the date that the written information security program was last approved by the Board of Directors:
[*FDIC Rules and Regulations Part 364 Appendix B Section III (A)(1)*]

b. Does your information security program contain written policies, procedures, and guidelines for securing, maintaining, and monitoring the following systems or platforms:
[*FFIEC IT Examination Handbook, Information Security Booklet*; *FIL-12-1999 Uniform Rating System for Information Technology*]

1. Core banking system (Y/N)?
2. Imaging (Y/N)?
3. Remote deposit capture (Y/N)?
4. Payment systems (including wire transfer and ACH) (Y/N)?
5. Voice over IP telephony (Y/N)?
6. Instant messaging (Y/N)?
7. Virtual private networking (Y/N)?
8. Wireless networking - LAN or WAN(Y/N)?
9. Local area networking (Y/N)?
10. Wide area networking (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. Portable devices such as PDAs, laptops, cell phones, etc. (Y/N)?
16. Other – please list:

c. Do you employ access controls on customer information systems (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(a); FFIEC IT Examination Handbook, Information Security Booklet; FIL-103-2005 Authentication in an Internet Banking Environment*]

d. Do you have a physical security program which defines and restricts access to information assets as well as protects against destruction, loss, or damage of customer information (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(b) and (h); FFIEC IT Examination Handbook, Information Security Booklet*]

e. Do you encrypt customer information (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(c); FFIEC IT Examination Handbook, Information Security Booklet*]

If "Yes," describe where encryption has been implemented:

f. Do you have formal configuration, change management, and patch management procedures for all applicable platforms identified in "b" above (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(d); FFIEC IT Examination Handbook, Information Security Booklet; FIL-43-2003 Guidance on Developing an Effective Software Patch Management Program*]

g. Does your information security program incorporate dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, customer information (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(e)*]

h. Do you have formal logging/monitoring requirements for platforms identified in "b" above (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(f); FFIEC IT Examination Handbook, Information Security Booklet*]

i. Do you have a formal intrusion detection program, other than basic logging, for monitoring host and/or network activity (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(f); FFIEC IT Examination Handbook, Information Security Booklet*]

j. Do you have an incident response plan defining responsibilities and duties for containing damage and minimizing risks to the institution and customers (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(g); FFIEC IT Examination Handbook, Information Security Booklet*]

   If "Yes," does the plan include customer notification procedures (Y/N)?
   [*FDIC Rules and Regulations Part 364 Appendix B, Supplement A; FIL-27-2005 Response Programs for Unauthorized Access to Customer Information and Customer Notice*]

k. Please provide the names and titles and/or committee members charged with formally overseeing and implementing the information security program:
[*FDIC Rules and Regulations Part 364 Appendix B Section II (A) and Section III (A)(2)*]

l. Do you maintain topologies, diagrams, or schematics depicting your physical and logical operating environment(s) (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (B); FFIEC IT Examination Handbook, Information Security Booklet*]

m. Do you have a process in place to monitor and adjust, as appropriate, the information security program (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (E)*]

n. Do you have an employee acceptable use policy (Y/N)?
[FDIC Rules and Regulations Part 364 Appendix B Section III (C)(2); FFIEC IT Examination Handbook, Information Security Booklet]

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

o. Do you have an employee security awareness training program (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(2); FFIEC IT Examination Handbook, Information Security Booklet*]

   If "Yes," please indicate the last date training was provided:

p. Does the bank report the overall status of the information security program and compliance with the Interagency Guidelines Establishing Information Security Standards to the Board or designated committee (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (F)*]

If "Yes," please provide the date that the findings were most recently approved by the Board of Directors.

q. Does the bank's strategic planning process incorporate information security (Y/N)?
[*FFIEC IT Examination Handbook, Management Booklet*]

r. Do you have policies/procedures for the proper disposal of customer and consumer information (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(4); FIL-7-2005 Fair and Accurate Credit Transactions Act of 2003 Guidelines Requiring the Proper Disposal of Consumer Information*]

s. Is a formal process in place to address changes to, or new issuance of, laws/regulations and regulatory guidelines (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (E); FFIEC IT Examination Handbook, Management Booklet*]

t. Have you experienced any material security incidents (internal or external) affecting the bank or bank customers since the prior FDIC IT examination (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(g); FIL-27-2005 Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*]

u. Do you serve as an Originating Depository Financial Institution (ODFI) (Y/N)?

If "Yes," do ACH policies/procedures address individual responsibilities, separation of duties, funds availability/credit limits, third-party agreements, information security, business continuity plans, insurance protections, and vendor management (Y/N)?
[*FFIEC IT Examination Handbook, Retail Payment Systems Booklet*]

v. If you serve as an ODFI, do all originators have direct agreements with your institution (Y/N)? (Y/N)?

If "No," are written agreements in place with third-party senders and/or third party service providers that address originator underwriting and liabilities (Y/N)?
[*FFIEC IT Examination Handbook, Retail Payment Systems Booklet, NACHA Rule Book*]

w. Do wire transfer policies/procedures address responsibilities and authorizations, separation of duties, funds availability/credit limits, information security, business continuity plans, insurance protections, and vendor management (Y/N)?
[*FFIEC IT Examination Handbook, Wholesale Payment Systems Booklet*]

x. Do you serve as a merchant acquirer for credit card activity (Y/N)?

If "Yes," do you have written policies/procedures that address merchant approval/termination, underwriting, fraud and credit monitoring, chargeback processing and control, and agent bank programs (Y/N)?

y. Are project management techniques and system development life cycle processes used to guide efforts at acquiring and implementing technology (Y/N)?
[*FFIEC IT Examination Handbook, Development and Acquisition Booklet; FIL-12-1999 Uniform Rating System for Information Technology*]

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 the IT auditor or employee performing internal IT audit functions (this may include outsourced internal control audits). Include who this person reports to, and a brief description of their education and experience conducting IT audits:
[*FDIC Rules and Regulations Part 364 Appendix A Section II (B) and Appendix B Section III (C)(3); FFIEC IT Examination Handbook, Audit Booklet*]

b. Do you have a written IT audit/independent review program that is based on the results of a risk analysis (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(3); FFIEC IT Examination Handbook, Audit Booklet*]

c. Please provide the following information regarding your most recent IT audits/independent reviews:
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(3) and (F); FFIEC IT Examination Handbook, Audit Booklet; FIL-12-1999 Uniform Rating System for Information Technology*]

	Audit Date	Entity Conducting Audit	Written Audit Report (Y/N)	Audit Committee/Board Review Date
Information Security Program				
IT General Controls Review				
Vulnerability Testing				
Penetration Testing				
Wire Transfer Audit				
NACHA Rule Compliance Audit				
Other:				
Other:				

d. Does audit coverage include a comparison of actual system configurations to documented/baseline configuration standards (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(3); FFIEC IT Examination Handbook, Information Security Booklet*]

e. Does audit coverage include assessing compliance with the information security program requirements (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(3); FFIEC IT Examination Handbook, Information Security Booklet*]

f. Does audit coverage include assessing users and system services access rights (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(3); FFIEC IT Examination Handbook, Information Security Booklet*]

g. Are the results of your audits/independent reviews used to adjust your risk assessment findings/results (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(3) and (E); FFIEC IT Examination Handbook, Information Security Booklet*]

h. Briefly describe any known conflicts or concentrations of duties:
[*FDIC Rules and Regulations Part 364 Appendix A Section II (B) and Appendix B Section III (C)(1)(e) and (3); FFIEC IT Examination Handbook, Audit Booklet*]

i. Do you have a system for tracking audit and regulatory exceptions to final resolution (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(3) and (E); FFIEC IT Examination Handbook, Audit Booklet*]

PART 4 - DISASTER RECOVERY AND BUSINESS CONTINUITY MANAGEMENT

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)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(h)*; *FFIEC IT Examination Handbook, Business Continuity Planning Booklet*]

If "Yes," please provide the name of your coordinator:

b. Are disaster recovery and business continuity programs based upon a business impact analysis (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(h); FFIEC IT Examination Handbook, Business Continuity Planning Booklet*]

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

c. Do you have formal agreements for an alternate processing site and equipment should the need arise to relocate operations (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(h)*; *FFIEC IT Examination Handbook, Business Continuity Planning Booklet*]

d. Do business continuity plans address procedures and priorities for returning to permanent and normal operations (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(h); FFIEC IT Examination Handbook, Business Continuity Planning Booklet*]

e. Do you maintain offsite backups of critical information (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(h)*; *FFIEC IT Examination Handbook, Business Continuity Planning Booklet*]

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

f. Do you have procedures for testing backup media at an offsite location (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(h); FFIEC IT Examination Handbook, Business Continuity Planning Booklet*]

g. Have disaster recovery/business continuity plans been tested (Y/N)?
[*FDIC Rules and Regulations Part 364 Appendix B Section III (C)(1)(h); FFIEC IT Examination Handbook, Business Continuity Planning Booklet*]

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

PART 5 – VENDOR MANAGEMENT AND SERVICE PROVIDER OVERSIGHT

Given the increased reliance on outside firms for technology-related products and services, please answer the following questions to help us assess the effectiveness of your vendor management and service provider oversight programs:

a. Does your vendor management program address due diligence, contract provision, financial condition, risk assessment, ongoing monitoring requirements, and third-party relationships such as subcontractors and agents (Y/N)?
[*FDIC Rules and Regulations 364 Appendix B Section III (D)*; *FIL-81-2000 Risk Management of Technology Outsourcing*]

b. Has the bank identified and reported its service provider relationships (both domestic and foreign-based) to the FDIC (Y/N)?
[*"Notification of Performance of Bank Services" FDIC Rules and Regulations 304.3 and 12USC1867 Section 7(c)(2) Bank Service Company Act (BCSA)*]

c. Are all of your direct or indirect service providers located within the United States (Y/N)?

   If "No," has management provided risk management policies; performance monitoring and oversight processes; legal and technical expertise; and access to critical, material, or sensitive customer information to address unique risks from these outsourcing relationships (Y/N)?
   [*FIL-52-2006 Foreign-Based Third-Party Service Providers Guidance on Managing Risks in These Outsourcing Relationships*]

d. Do licensing agreements for core processing or mission-critical applications require vendors to maintain application software so that the software operates in compliance with all applicable federal and state regulations (Y/N)?
[*FIL-121-2004 Computer Software Due Diligence Guidance on Developing an Effective Computer Software Evaluation Program to Assure Quality and Regulatory Compliance*]

e. Do you require your service providers by contract to implement measures designed to meet the objectives of the Interagency Guidelines Establishing Information Security Standards (Y/N)?
[*FDIC Rules and Regulations 364 Appendix B Section III (D)(2)*]

f. Where indicated by the risk assessment, do you review audits, summaries of test results, and other equivalent evaluations of your service providers to confirm that they are fulfilling contractual obligations to implement appropriate measures designed to meet the objectives of the Interagency Guidelines Establishing Information Security Standards (Y/N)?
[*FDIC Rules and Regulations 364 Appendix B Section III (D)(3)*]

Clarifying or Additional Comments

Applicable ITOQ items	*The IT Officer's Questionnaire addresses information security programs from a multi-disciplinary enterprise-wide approach. Many of the questions may be used to help identify compliance with Part 364, Appendix B, of the FDIC Rules and Regulations. The following chart can be used as a guide in conducting self assessments.* ***Interagency Guidelines Establishing Information Security Standards***
	II. Standards for Information Security
2a 2k	A. Information Security Program. Each bank shall implement 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. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.
qualitative	B. Objectives. A bank's information security program shall be designed to: 1. Ensure the security and confidentiality of customer information; 2. Protect against any anticipated threats or hazards to the security or integrity of such information; 3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and 4. Ensure the proper disposal of customer information and consumer information.
	III. Development and Implementation of Information Security Program
1a 1b 1i 2a 2k	A. Involve the **Board of Directors**. The Board of Directors or an appropriate committee of the Board of each bank shall: 1. Approve the bank's written information security program; and 2. Oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.
1c-1f 2l	B. **Assess Risk**. Each bank shall: 1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems. 2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information. 3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.
1g 2a	C. **Manage and Control Risk**. Each bank shall: 1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:
2c	**a.** Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means. [*FIL-103-2005 Authentication in an Internet Banking Environment*]

2d	b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;
2e	c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
1h 2f	d. Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;
2g 3h	e. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;
2h 2i	f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;
2j 2t	g. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; [*FIL-27-2005 Response Programs for Unauthorized Access to Customer Information and Customer Notice*]and
2d 4a-4g	h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.
2n 2o	2. Train staff to implement the bank's information security program.
3a-3i	3. Regularly **test the key controls**, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.
2r	4. Develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of customer information and consumer information in accordance with each of the requirements of this paragraph III.
5a 5e 5f	D. Oversee **Service Provider** Arrangements. Each bank shall: 1. Exercise appropriate due diligence in selecting its service providers; 2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and 3. Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.
1h 1k 2m 3g 3i	E. Adjust the Program. Each bank shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.
1i 1j 2p 3c	F. **Report to the Board**. Each bank shall report to its board or an appropriate committee of the Board at least annually. This report should describe the overall status of the information security program and the bank's compliance with these Guidelines. The report, which will vary depending upon the complexity of each bank's program should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations, and management's responses; and recommendations for changes in the information security program.