Baseline Nonbank Cybersecurity Exam Program

Version 1.1
Released Date: 06/30/2023

Exam Program Summary: This information technology (IT) and cybersecurity exam program was created by state regulators for examinations of nonbank institutions. The procedures provide a high-level risk evaluation of the four critical components of the Uniform Rating System for Information Technology (URSIT) which include Audit, Management, Development and Acquisition, and Support and Delivery. URSIT was developed by the Federal Financial Institutions Examination Council (FFIEC) to evaluate the information technology function at banking institutions. The primary purpose of this rating system is to evaluate the examined institution's overall risk exposure and risk management performance and determine the degree of supervisory attention necessary to ensure that weaknesses are addressed and risks are properly managed.

The exam program should be used as a baseline review of smaller, noncomplex, low risk institutions. The program is targeted for use by examiners with or without specialized IT and cybersecurity knowledge.

Question Numbering: The questions are numbered in the following format: baseline number / enhanced exam program number. The format allows the user to easily track the question number in the baseline exam program while having access to the corresponding question number in the enhanced exam program.

Table of Contents

AUDIT		
Question Details	**Baseline Examination Questions**	**Examiner Notes**
1/Audit-01 Request List: IT-8 FTC Citation: 16 CFR 314.4(d)(1)	Is the technology audit function appropriate for the size and complexity of the institution? Consider: • Independence – managed by personnel independent of daily operations for areas covered in the audit scope; • Risk Assessment Process – used to set the scope and frequency; • Issue Tracking Process – documented and reviewed periodically by the board or a committee appointed by the board; and • Auditor Expertise and Training - sufficient for the complexity of the function in relation to the technology and overall risk at the institution.	

DEVELOPMENT & ACQUISITION		
Question Details	**Baseline Examination Questions**	**Examiner Notes**
2/D&A-01 Request List: IT-1, IT-7 FTC Citation: 16 CFR 314.4(c)(4)	Does the institution have a formal written policy or methodology to guide how information systems are approved, prioritized, acquired, developed, and maintained?	
3/D&A-05 Request List: IT-1, IT-7 FTC Citation: 16 CFR 314.4(c)(7)	Does the institution have a change management program to document, track, test, authorize, approve, and perform system and environmental changes?	
4/D&A-06 Request List: IT-1, IT-7	Are end-of-life assets identified with an adequate replacement schedule?	

MANAGEMENT		
Question Details	**Baseline Examination Questions**	**Examiner Notes**
5/MGMT-01 Request List: IT-3 FTC Citation: 16 CFR 314.4(e)(2)	Does the institution have dedicated cybersecurity resources with appropriate job titles and areas of responsibility?	
6/MGMT-03 Request List: IT-1(c) FTC Citation: 16 CFR 314.4(e)	Does management have a program to ensure employees are up to date with emerging issues and technologies?	
7/MGMT-04 Request List: IT-3(d)	Is succession planning in place for key IT personnel?	
8/MGMT-05 Request List: IT-2(a)	Is technology sufficiently addressed in the institution's overall strategic planning and budgeting processes?	
9/MGMT-06 Request List: IT-1 FTC Citation: 16 CFR 314.3(b)	Is the information security program formally documented and reasonably designed to accomplish the following objectives? • Ensure the security and confidentiality of customer information; • Protect against any anticipated threats or hazards to the security or the integrity of such information; and • Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.	
10/MGMT-07 Request List: IT-2(d) FTC Citation: 16 CFR 314.4(a)	Who develops, reviews, and manages the information security program? The board is required to designate an individual(s) to oversee, implement, and enforce the information security program (known as the "Qualified Individual"). *The Qualified Individual may be employed by the entity, an affiliate, or a service provider. Document the designated name(s) and contact information.*	

MANAGEMENT		
16 CFR 314.4(e)(2)		
11/MGMT-09 Request List: IT-1 FTC Citation: 16 CFR 314.3(a)	Do policies and procedures that comprise the information security program adequately document all relevant areas?	
12/MGMT-10 Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(8)	Is all user activity monitored in accordance with an Acceptable Use Policy?	
13/MGMT-11 Request List: IT-1	Is there a clean desk policy in place that includes securely storing sensitive papers and mobile devices, clearing off desks at the end of each day, and locking file cabinets?	
14/MGMT-13 Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(6)	Are written policies and procedures in place for secure destruction and disposal of physical and electronic records of sensitive information?	
15/MGMT-20 Request List: IT-2(b), IT-2(c)	Does executive management and/or the board receive regular briefings on relevant information security threats and institutional metrics?	
16/MGMT-21 Request List: IT-2 FTC Citation: 16 CFR 314.4(i) *	Does the Qualified Individual report to the board in writing at least annually the following information: • Overall status of the information security program and compliance with 16 CFR, Part 314; and • Material matters related to the information security program, such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's	

* *Per 16 CFR 314.6, Sections 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.*

MANAGEMENT		
	responses thereto, and recommendations for changes in the information security program.	
17/MGMT-22 Request List: IT-1(b) FTC Citation: 16 CFR 314.4(b) *	Is there a documented risk assessment process that includes the following? • Asset identification; • Risk identification; • Risk assessment and measurement: analyze the risk (likelihood/impact on specific assets) and rank/measure risk (high, medium, or low for likelihood/impact) with definitions; • Risk mitigation: identify and prioritize ways to reduce risks and describe how identified risks will be mitigated or accepted; and • Risk monitoring.	
18/MGMT-32 Request List: IT-5, IT-8 FTC Citation: 16 CFR 314.4(d) *	Is the effectiveness of key controls identified during the risk assessment process regularly tested or monitored, such as through the IT audit process and network penetration testing and scanning?	
19/MGMT-33 Request List: IT-1(c) FTC Citation: 16 CFR 314.4(e)	Is information security awareness training provided to all employees regardless of level, contractors, and vendors as part of initial training for new users and annually thereafter?	
20/MGMT-37 Request List: IT-9 FTC Citation: 16 CFR 314.4(f)	Is the institution's vendor management/third-party risk program documented and sufficient to ensure that it employs trustworthy third parties? The program should include the following components: • Due diligence process for new vendors, including cloud vendors; • Ongoing monitoring process for existing vendors in consideration of the confidentiality, availability, and integrity of information stored with the vendor; • Contractual requirements for all vendors; • Incident response and notification practices to both consumers and the institution; and • Cloud vendors.	

* *Per 16 CFR 314.6, Sections 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.*

MANAGEMENT		
21/MGMT-46 Request List: IT-14	Does the institution have insurance policies that cover cybersecurity areas such as information security and incident response? *Note: Cybersecurity insurance is optional, but institutions should consider whether cybersecurity insurance would be an effective part of the overall risk management programs.*	

SUPPORT & DELIVERY		
Question Details	**Baseline Examination Questions**	**Examiner Notes**
22/S&D-01 Request List: IT-4(a), IT-15 FTC Citation: 16 CFR 314.4(c)(2)	Does the institution have an acceptable up-to-date network topology (diagram) available for review? Consider the following: • Locations of servers; • Locations of clusters that specify the virtual machines associated with the host; • Network connections to the internet; • User devices, either individually or as a group; • Devices or servers that provide key network services such as DNS and DHCP or core applications; • DMZ areas; • Where data is stored; • VLANS; • Wireless networks; • Cloud resources; • VPN connections to service providers; and • Remote access entry points for users or vendors (VPN connections).	
23/S&D-04 Request List: IT-4(a) FTC Citation: 16 CFR 314.4(c)(8)	Does the institution have a firewall(s) that is monitored with the firewall rules regularly reviewed to determine whether they are still required from a business perspective?	
24/S&D-10 Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(3)	Is encryption used to secure data at rest and/or in motion?	

SUPPORT & DELIVERY		
25/S&D-22 Request List: IT-1, IT-5 FTC Citation: 16 CFR 314.4(c)(8)	Is an intrusion detection/prevention system (IDS/IPS) in use?	
26/S&D-23 Request List: IT-1, IT-5 FTC Citation: 16 CFR 314.4(c)(8)	If an IDS/IPS is used, who is responsible for reviewing and monitoring the IDS/IPS event reports?	
27/S&D-26 Request List: IT-1, IT-5	Is malware protection (e.g., antivirus) deployed on all workstations and servers?	
28/S&D-27 Request List: IT-1, IT-5	How is malicious code protection deployed, updated, and managed?	
29/S&D-34 Request List: IT-6 FTC Citation: 16 CFR 314.4(c)(2)	What is the institution's process for applying security patches for organizational assets?	
30/S&D-35 Request List: IT-6 FTC Citation: 16 CFR 314.4(c)(2)	Are patch status reports generated and independently reviewed to validate the effectiveness of the patch management program?	
31/S&D-36 Request List: IT-6	Are automated systems used to identify and patch systems?	

SUPPORT & DELIVERY		
32/S&D-42 Request List: IT-4(a), IT-4(c), IT-14 FTC Citation: 16 CFR 314.4(c)(2)	Does the institution maintain an inventory of all approved hardware and software assets? If yes, request a copy and verify that it generally matches the topography diagram.	
33/S&D-45 Request List: IT-5(b), IT-5(c) FTC Citation: 16 CFR 314.4(d)(2) *	Are vulnerability scans conducted? If yes, indicate by whom, frequency, and what exactly is scanned.	
34/S&D-48 Request List: IT-5(c) FTC Citation: 16 CFR 314.4(d)(2) *	Are penetration tests conducted? If yes, indicate by whom and frequency.	
35/S&D-49 Request List: IT-1, IT-12, IT-13 FTC Citation: 16 CFR 314.4(c)(1) 16 CFR 314.4(c)(5)	Has the entity implemented multi-factor authentication (MFA) or, alternatively, approved in writing, reasonable equivalent controls for any individual accessing any information system? When evaluating alternative controls, consider the following: • Password length, complexity, expiration, and reuse requirements; • Changing default/factory password settings; • Screen lock after inactivity periods; • Lockouts after incorrect login tries; • Help desk procedures to deal with failed login attempts; • No shared accounts; • Access limited to business need/least privilege;	

* *Per 16 CFR 314.6, Sections 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.*

SUPPORT & DELIVERY		
	• Administrative privileges only assigned when needed; and • Remote access procedures.	
36/S&D-54 Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(1)	Are all user access levels (including administrators) monitored and reviewed regularly?	
37/S&D-55 Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(1)	Is there an employee departure checklist used to ensure all user accounts are disabled for employees who have left the institution or changed job responsibilities?	
38/S&D-56 Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(1) 16 CFR 314.4(c)(2)	Determine the adequacy of controls in place for company-issued or personal mobile devices. Consider: • Types of data accessed or stored • Patch management processes • Security auditing and monitoring capabilities • Anti-virus and anti-malware • Remote wipe capabilities • Drive encryption • Secure wireless networks/connections or VPN usage	

SUPPORT & DELIVERY		
39/S&D-68 Request List: IT-1, IT-11 FTC Citation: 16 CFR 314.3(a) 16 CFR 314.3(b)	Is the business continuity management process documented and appropriate for the size and complexity of the institution? Consider the following: • Plans are based on appropriate business impact analysis(es). • Plans are based on appropriate risk assessment(s). • Plans effectively address pandemic issues. • Plans identify essential business functions and associated contingency requirements. • Plans provide recovery objectives and restoration priorities. • Plans include contingency locations so employees can continue to work. • Plans address responsibilities and decision-making authorities for designated teams and/or staff members with contact information. • Plans include communication procedures for contacting, employees, vendors, regulators, municipal authorities, emergency response personnel, and customers.	
40/S&D-69 Request List: IT-2 FTC Citation: 16 CFR 314.4(g)	Are business continuity and disaster recovery plans reviewed at least annually after implementation and updated when necessary?	
41/S&D-71 Request List: IT-11(e) FTC Citation: 16 CFR 314.4(d)(1)	Are business continuity and disaster recovery plans appropriately tested regularly?	
42/S&D-72 Request List: IT-11(e) FTC Citation: 16 CFR 314.4(d)(1)	Does testing include both systems and personnel using different testing methods such as failovers and tabletop testing?	

SUPPORT & DELIVERY		
43/S&D-75 Request List: IT-11(e) FTC Citation: 16 CFR 314.4(g)	Are remediation plans to address gaps identified during the testing of business continuity and disaster recovery plans developed, tracked, and regularly reviewed?	
44/S&D-76 Request List: IT-11(b) FTC Citation: 16 CFR 314.4(c)(2)	Does the institution have a data backup program in place?	
45/S&D-77 Request List: IT-11(b) FTC Citation: 16 CFR 314.4(c)(2) 16 CFR 314.4(d)(1)	Is data backed up regularly and tested?	
46/S&D-78 Request List: IT-11(b)	Is data stored offline to mitigate the risk of a ransomware attack on the online backup?	
47/S&D-79 Request List: IT-11(b	Can the institution successfully restore information and resume business operations from backups? Indicate the date this was last tested.	
48/S&D-84 Request List: IT-1,IT-10 FTC Citation: 16 CFR 314.4(h) *	Does the institution have an incident response plan that establishes specific procedures for different types of incidents?	

* *Per 16 CFR 314.6, Sections 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.*

SUPPORT & DELIVERY		
49/S&D-85 Request List: IT-1, IT-10 FTC Citation: 16 CFR 314.4(h) *	Does the incident response plan address responsibilities and decision-making authorities for designated teams and/or staff members?	
50/S&D-86 Request List: IT-1, IT-10 FTC Citation: 16 CFR 314.4(h) *	Does the incident response plan include guidelines for notifying customers, law enforcement, vendors, and regulatory agencies when the institution becomes aware of an incident involving the unauthorized access to or use of sensitive customer information? The entity should be aware of reporting requirements enacted by state and federal laws or regulations specific to the business.	
51/S&D-93 Request List: IT-10(b) FTC Citation: 16 CFR 314.4(d)(1) 16 CFR 314.4(h)(7) *	Is the incident response plan reviewed, tested, and updated regularly? Consider the following: • Reviews and updates performed after every security incident; and • Reviews and tests performed annually, at a minimum.	
52/S&D-94 Request List: IT-1, IT-10 FTC Citation: 16 CFR 314.4(c)(8)	Are information systems monitored for potential anomalies or security incidents?	
53/S&D-95 Request List: IT-1, IT-10	Are event logs collected or stored in a centralized location for later review?	
54/S&D-96 Request List: IT-10(c)	When was the last time an incident occurred? Indicate the date and how the institution handled it.	

* *Per 16 CFR 314.6, Sections 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.*