Enhanced Nonbank Cybersecurity Exam Program

Version 1.1
Released Date: 10/21/2024

Exam Program Summary: This information technology (IT) and cybersecurity exam program was created by state regulators for examinations of nonbank institutions. The procedures provide an in-depth 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.

This exam program includes the baseline procedures (noted by a light blue shading), plus additional procedures and should be used to provide a more in-depth review for larger, more complex institutions or for those where concerns are raised during the exam. The program is targeted for use by examiners with specialized knowledge of IT and cybersecurity.

Table of Contents

AUDIT		
Question Details	**Enhanced Examination Questions**	**Examiner Notes**
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.	
Audit-02.EN Request List: IT-8(a), IT-8(g) FTC Citation: 16 CFR 314.4(d)(1)	Who conducts the technology audits?	
Audit-03.EN Request List: IT-8(d) FTC Citation: 16 CFR 314.4(d)(1)	If technology audits are outsourced, does the contract/engagement letter cover expectations and responsibilities for both parties; scope, timeframes, and cost of work; and institution access to workpapers?	
Audit-04.EN Request List: IT-8(c) FTC Citation: 16 CFR 314.4(d)(1)	Is a risk assessment used to determine required audit frequency and scope?	
Audit-05.EN Request List: IT-8(c) FTC Citation: 16 CFR 314.4(d)(1)	Do audit results influence successive risk assessments?	

AUDIT		
Question Details	**Enhanced Examination Questions**	**Examiner Notes**
Audit-06.EN Request List: IT-8(a), IT-8(b), IT-8(c) FTC Citation: 16 CFR 314.4(d)(1)	How frequently are audits conducted?	
Audit-07.EN Request List: IT-8(b), IT-8(c) FTC Citation: 16 CFR 314.4(d)(1)	Does the actual frequency align with the risk assessment?	
Audit-08.EN Request List: IT-8(c) FTC Citation: 16 CFR 314.4(d)(1)	Does the risk assessment cover the entire technology audit universe?	
Audit-09.EN Request List: IT-8(c) FTC Citation: 16 CFR 314.4(d)(1)	Does the audit plan adequately address technology risk exposure throughout the institution and its service providers?	
Audit-10.EN Request List: IT-8(g) FTC Citation: 16 CFR 314.4(d)(1)	Is the technology audit function independent of daily operations for areas covered in the audit scope?	
Audit-11.EN Request List: IT-8(f)	Is there a process for tracking issues identified during the risk assessment process, monitoring, auditing, and regulatory examinations?	

AUDIT		
Question Details	**Enhanced Examination Questions**	**Examiner Notes**
FTC Citation: 16 CFR 314.4(d)(1)		
Audit-12.EN Request List: IT-8(f) FTC Citation: 16 CFR 314.4(d)(1)	Does the tracking list assign the action needed to correct the issue and record when the issue is resolved, or the risk accepted?	
Audit-13.EN Request List: IT-2 FTC Citation: 16 CFR 314.4(d)(1)	Are audit results and issue remediation progress reviewed by the board or an appropriate committee of the board?	

DEVELOPMENT & ACQUISITION		
Question Details	**Enhanced Examination Questions**	**Examiner Notes**
D&A-01 Request List: IT-1, IT-7 FTC Citation: 16 CFR 314.3(a)	Does the institution have a formal written policy or methodology to guide how information systems are approved, prioritized, acquired, developed, and maintained?	
D&A-02.EN Request List: IT-1, IT-7	Is all hardware maintenance work authorized, tracked, and reviewed?	
D&A-03.EN Request List: IT-1, IT-7 FTC Citation: 16 CFR 314.4(c)(4)	If the institution develops their own software, do they follow a documented software development life cycle?	
D&A-04.EN	If the institution does internal development, do they perform application security testing?	

DEVELOPMENT & ACQUISITION		
Request List: IT-1, IT-7 FTC Citation: 16 CFR 314.4(c)(4)		
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?	
D&A-06 Request List: IT-1, IT-7	Are end-of-life assets identified with an adequate replacement schedule?	

MANAGEMENT		
Question Details	**Enhanced Examination Questions**	**Examiner Notes**
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?	
MGMT-02 Request List: IT-1(c) FTC Citation: 16 CFR 314.4(e)(3) 16 CFR 314.4(e)(4)	Does management have a program to ensure all information security personnel, including key personnel, are kept up to date with respect to changing information security threats and countermeasures?	
MGMT-03 Request List: IT-3(d)	Is succession planning in place for key IT personnel?	
MGMT-04	Is technology sufficiently addressed in the institution's overall strategic planning and budgeting processes?	

MANAGEMENT		
Request List: IT-2(a)		
MGMT-05 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.	
MGMT-06 Request List: IT-2(d) FTC Citation: 16 CFR 314.4(a) 16 CFR 314.4(e)(2)	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.*	
MGMT-07.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(g)	When was the last time the information security program was updated in response to the results of testing and monitoring, changes to operations or business arrangements, risk assessments, or any other known circumstance that may have a material impact on the program?	
MGMT-08 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?	
MGMT-09.EN Request List: IT-1	Are all policies reviewed regularly and dated?	

MANAGEMENT		
FTC Citation: 16 CFR 314.3(a)		
MGMT-10.EN Request List: IT-2	Are all policies, plans, and programs presented to executive management and/or the board for approval?	
MGMT-11.EN Request List: IT-1	Does the institution periodically compare written policies and procedures with actual implementation of those policies and procedures?	
MGMT-12.EN Request List: IT-1	Who identifies risk and develops metrics to measure policy compliance?	
MGMT-13 Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(8)	Is all user activity monitored in accordance with an Acceptable Use Policy?	
MGMT-14.EN Request List: IT-1	Are personnel with authority to access customer information and confidential institution information required to sign and abide by a confidentiality agreement and/or an acceptable use agreement?	
MGMT-15 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?	
MGMT-16.EN Request List: Observe	Is the clean desk policy enforced?	
MGMT-17 Request List: IT-1	Are written policies and procedures in place for secure destruction and disposal of physical and electronic records of sensitive information?	

MANAGEMENT		
FTC Citation: 16 CFR 314.4(c)(6)		
MGMT-18.EN Request List: Observe FTC Citation: 16 CFR 314.4(c)(6)	Are shred bins locked and not overflowing?	
MGMT-19.EN Request List: Observe FTC Citation: 16 CFR 314.4(c)(6)	If a third-party shredding institution is used, are the documents shredded onsite and/or transported securely?	
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?	
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 responses thereto, and recommendations for changes in the information security program.	
MGMT-22 Request List: IT-1(b)	Is there a documented risk assessment process that includes the following? • Asset identification; • Risk identification;	

[*] *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		
FTC Citation: 16 CFR 314.4(b) [*]	- 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.	
MGMT-23.EN[*] Request List: IT-1(b) FTC Citation: 16 CFR 314.4(b)	Is the risk assessment: - Formal; - Proactive; - Ongoing; - Understood and supported by executive management and the board; - Linked to goals and objectives; and - Institution-wide.	
MGMT-24.EN[*] Request List: IT-1(b) FTC Citation: 16 CFR 314.4(b)(1) 16 CFR 314.4(c)(2)	Has data been classified based on the criticality/sensitivity of the information and determined and documented for what information needs to be protected and secured?	
MGMT-25.EN[*] Request List: IT-1(b), IT-4 FTC Citation: 16 CFR 314.4(b)(1)	Does the risk assessment include all information systems, including network and software design as well as information processing, storage, transmission, and disposal?	

[*] *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.

[*] *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.

[*] *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.

[*] *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		
MGMT-26.EN[*] Request List: IT-1(b) FTC Citation: 16 CFR 314.4(b)	Are inherent and residual risks identified by the institution?	
MGMT-27.EN[*] Request List: IT-1(b) FTC Citation: 16 CFR 314.4(b)	Does the risk assessment consider failures of employee training and management?	
MGMT-28.EN[*] Request List: IT-1(b) FTC Citation: 16 CFR 314.4(b)	Does the risk assessment consider the threat of attacks, intrusions, and/or other system failures?	
MGMT-29.EN[*] Request List: IT-1(b) FTC Citation: 16 CFR 314.4(b)	Does the risk assessment include administrative, technical, and physical controls?	
MGMT-30.EN[*]	Is the risk assessment updated regularly to include new technologies, products, and services?	

[*] *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.

[*] *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.

[*] *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.

[*] *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.

[*] *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		
Request List: IT-1(b) FTC Citation: 16 CFR 314.4(b)(2)		
MGMT-31.EN[*] Request List: IT-2 FTC Citation: 16 CFR 314.4(b)	How frequently does executive management and/or the board review the institution's risk thresholds and approve the risk assessment?	
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?	
MGMT-33 Request List: IT-1(c) FTC Citation: 16 CFR 314.4(e)(1)	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?	
MGMT-34.EN Request List: IT-1(c)	Is information security awareness training monitored and tracked to ensure all required personnel complete the training?	
MGMT-35.EN	Do users confirm they understand the training material and is the confirmation documented?	

[*] *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.

[*] *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		
Request List: IT-1(c)		
MGMT-36.EN Request List: IT-1(c)	Is security awareness training updated and revised as needed?	
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.	
MGMT-38.EN Request List: IT-9 FTC Citation: 16 CFR 314.4(f)(1)	Does the institution perform due diligence before entering into a contract?	
MGMT-39.EN Request List: IT-9 FTC Citation: 16 CFR 314.4(f)(3)	Is an ongoing monitoring program in place with frequency determined by the confidentiality, availability, and integrity of information stored with the vendor?	
MGMT-40.EN	Do monitoring processes include evaluating the vendor's incident response practices and contractual notification requirements to both consumers and the institution?	

MANAGEMENT		
Request List: IT-9 FTC Citation: 16 CFR 314.4(f)(3)		
MGMT-41.EN Request List: IT-9 FTC Citation: 16 CFR 314.4(f)(2)	Is the vendor required to report security incidents that directly impact the institution and/or the institution's customers to the institution?	
MGMT-42.EN Request List: IT-9 FTC Citation: 16 CFR 314.4(f)(2)	Are contracts in place with all vendors that include specified contract deliverables, due dates, and service level agreements?	
MGMT-43.EN Request List: IT-9 FTC Citation: 16 CFR 314.4(f)(2)	Are security responsibilities documented for both the institution and the vendor?	
MGMT-44.EN Request List: IT-9 FTC Citation: 16 CFR 314.4(f)(2)	Do vendor contracts require service providers to implement and maintain appropriate information security safeguards?	
MGMT-45.EN Request List: IT-9	Are cloud vendors included in the vendor management program and adequately monitored and reviewed?	

MANAGEMENT		
FTC Citation: 16 CFR 314.4(f)		
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.*	
MGMT-47.EN Request List: IT-14	Has the institution ever applied for and been rejected from any cyber or IT-related insurance policies?	
MGMT-48.EN Request List: IT-14	Has the institution ever received any payouts related to a cyber insurance policy or associated event?	

SUPPORT & DELIVERY		
Question Details	**Enhanced Examination Questions**	**Examiner Notes**
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).	
S&D-02.EN Request List: IT-4(a)	Are the network services segregated to ensure data integrity and security?	

SUPPORT & DELIVERY		
FTC Citation: 16 CFR 314.4(c)(2)		
S&D-03.EN Request List: IT-4(a) FTC Citation: 16 CFR 314.4(c)(2)	Are any servers that communicate directly with the internet or other untrusted network segmented from the internal network in a DMZ?	
S&D-04 Request List: IT-4(a) FTC Citation: 16 CFR 314.4(c)(1)	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?	
S&D-05.EN Request List: IT-4(a)	What firewall approach is used: whitelisting or blacklisting?	
S&D-06.EN Request List: IT-4(a)	Is the firewall policy restrictive by default?	
S&D-07.EN Request List: IT-4(a)	Does the institution have a specific business reason for each firewall rule?	
S&D-08.EN Request List: IT-4(a) FTC Citation: 16 CFR 314.4(c)(3)	Are wireless network(s) secured using acceptable encryption standards?	
S&D-09.EN Request List: IT-4(a)	Does the public have access to the institution's wireless network(s)?	
S&D-10 Request List: IT-1	Is encryption used to secure data at rest and/or in motion?	

SUPPORT & DELIVERY		
FTC Citation: 16 CFR 314.4(c)(3)		
S&D-11.EN Request List: IT-4(a) FTC Citation: 16 CFR 314.4(c)(8)	Is a Data Loss/Leak Protection (DLP) solution in place on the network?	
S&D-12.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(2)	Are controls in place to manage the use of removable media devices?	
S&D-13.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(2)	How does the institution protect information transmitted by printers, fax machines, etc.?	
S&D-14.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(3)	Is sensitive information sent between the institution and customers securely?	
S&D-15.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(3)	Is sensitive information sent between the institution and third parties securely?	
S&D-16.EN Request List: IT-1	Does the institution caution customers against sending sensitive information through unsecured channels?	

SUPPORT & DELIVERY		
S&D-17 Request List: IT-1, IT-10 FTC Citation: 314.4(d)(1) 314.4(d)(2) [*]	Are information systems monitored for potential anomalies or security incidents?	
S&D-18.EN Request List: IT-1, IT-5 FTC Citation: 314.4(d)(1) 314.4(d)(2) [*]	Is detection and monitoring of system activity and security incidents performed internally under the direction of the Qualified Individual or externally by a third party?	
S&D-19.EN Request List: IT-1, IT-5 FTC Citation: 314.4(d)(1) 314.4(d)(2) [*]	Is system activity and information security event monitoring performed by the institution sufficient? Describe monitoring processes. Consider the following: • Online actions including time stamps; • Unsuccessful login attempts; • Similar website names; • Employee and vendor user activity in accordance with the Acceptable Use Policy; and • Tampering (e.g., actions conducted online, time stamps of actions conducted online, unsuccessful login attempts, who enters/exits the building, etc.).	
S&D-20.EN Request List: IT-1, IT-5 FTC Citation: 314.4(d)(1) 314.4(d)(2) [*]	Has sufficient audit logging been enabled on all systems and networking devices? Consider the following: • Audit log review frequencies; • Extent automated log file analysis tools are used; • Automated real-time alerts of suspicious behavior; and • Length of time audit logs are maintained.	

[*] *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.

[*] *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.

[*] *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.

[*] *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		
S&D-21 Request List: IT-1, IT-5 FTC Citation: 16 CFR 314.4(c)	Is an intrusion detection/prevention system (IDS/IPS) in use?	
S&D-22 Request List: IT-1, IT-5 FTC Citation: 16 CFR 314.4(c)	If an IDS/IPS is used, who is responsible for reviewing and monitoring the IDS/IPS event reports?	
S&D-23.EN Request List: IT-1, IT-5	If an IDS/IPS is used, what design type is being used (i.e., signature-based, anomaly-based, or a combination of the two)?	
S&D-24.EN Request List: IT-1, IT-5	Are IDS/IPS signatures reviewed regularly?	
S&D-25 Request List: IT-1, IT-5 FTC Citation: 16 CFR 314.4(c)	Is malware protection (e.g., antivirus) deployed on all workstations and servers?	
S&D-26 Request List: IT-1, IT-5 FTC Citation: 16 CFR 314.4(c)	How is malicious code protection deployed, updated, and managed?	
S&D-27.EN Request List: IT-1, IT-5 FTC Citation: 16 CFR 314.4(c)	Do malware detection scans on workstations occur regularly on a pre-defined basis?	

SUPPORT & DELIVERY		
S&D-28.EN Request List: IT-1, IT-5 FTC Citation: 16 CFR 314.4(c)	Are incoming e-mail attachments automatically scanned by the desktop malware solution prior to download?	
S&D-29.EN Request List: IT-1, IT-5 FTC Citation: 16 CFR 314.4(c)	Does the institution use spam filtering software to reduce the number of unsolicited emails?	
S&D-30.EN Request List: IT-1, IT-5 FTC Citation: 16 CFR 314.4(c)	Does the institution use web filtering to prevent employees from visiting dangerous websites?	
S&D-31.EN Request List: IT-1, IT-5 FTC Citation: 16 CFR 314.4(c)	Does the institution use pop-up blockers to eliminate/reduce the amount of unsolicited pop-up advertisements on the internet?	
S&D-32.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(c)	Are employees permitted to use their personal email accounts for business communications?	
S&D-33 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?	

SUPPORT & DELIVERY		
S&D-34 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?	
S&D-35 Request List: IT-6	Are automated systems used to identify and patch systems?	
S&D-36.EN Request List: IT-5, IT-6 FTC Citation: 16 CFR 314.4(c)(2)	Have all security patches been applied to institutional assets?	
S&D-37.EN Request List: IT-5, IT-6 FTC Citation: 16 CFR 314.4(c)(2)	Are new patches regularly applied as they become available?	
S&D-38.EN Request List: IT-6 FTC Citation: 16 CFR 314.4(c)(2)	Is there a specific test environment set up separate from the production environment to allow for testing patches and updates without destroying or damaging critical data?	
S&D-39.EN Request List: IT-5, IT-6 FTC Citation: 16 CFR 314.4(c)(2)	How does the institution verify patches and updates were successfully installed on all assets?	
S&D-40.EN Request List: IT-1, IT-6	Is there a process for applying patches to dormant machines?	

SUPPORT & DELIVERY		
FTC Citation: 16 CFR 314.4(c)(2)		
S&D-41 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.	
S&D-42.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(2)	Is all software on the network actively managed, inventoried, and tracked so that only authorized software is installed and can execute?	
S&D-43.EN Request List: IT-4(b) FTC Citation: 16 CFR 314.4(c)(2)	Does the institution have an up-to-date data flow diagram that shows the flow and storage of PII data throughout its lifecycle?	
S&D-44 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.	
S&D-45.EN Request List: IT-5(b), IT-5(c)	Do network vulnerability scanning tools detect wireless access points connected to the wired network?	

[*] *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		
FTC Citation: 16 CFR 314.4(d)(2) [*]		
S&D-46.EN Request List: IT-5(b), IT-5(c), IT-5(d) FTC Citation: 16 CFR 314.4(c)(1)	Are unauthorized or rogue access points deactivated?	
S&D-47 Request List: IT-5(c) FTC Citation: 16 CFR 314.4(d)(2) [*]	Are penetration tests conducted? If yes, indicate by whom and frequency.	
S&D-48 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; • Administrative privileges only assigned when needed; and • Remote access procedures.	
S&D-49.EN	If remote access is allowed using laptops and other mobile devices, does the institution use a network access control solution?	

[*] *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.

[*] *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		
Request List: IT-1, IT-13 FTC Citation: 16 CFR 314.4(c)(1)		
S&D-50.EN Request List: IT-1, IT-13 FTC Citation: 16 CFR 314.4(c)(5)	Does remote access for employees, board members, customer accounts, and vendors require the use of multi-factor authentication?	
S&D-51.EN Request List: IT-1, IT-13 FTC Citation: 16 CFR 314.4(c)(3)	Is encryption implemented on the remote access solution if remote users can access or retrieve sensitive or confidential information residing in the internal network?	
S&D-52.EN Request List: IT-1, IT-13 FTC Citation: 16 CFR 314.4(c)(8)	How is remote access monitored?	
S&D-53 Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(1)	Are all user access levels, including administrators, monitored, and reviewed regularly?	
S&D-54 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?	
S&D-55	Determine the adequacy of controls in place for company-issued or personal mobile devices. Consider:	

SUPPORT & DELIVERY		
Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(1) 16 CFR 314.4(c)(2)	• 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	
S&D-56.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(1) 16 CFR 314.4(c)(2)	If the institution permits Bring Your Own Device (BYOD), are controls adequate? Consider the following: • Levels of permission and access (i.e., what apps are available to which roles); • If devices locally store information or just view it; • An inventory of BYOD devices and what information is stored and accessed on each; and patching and updating devices.	
S&D-57.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(c)	Is the BYOD program managed by an automated Mobile Device Management (MDM) solution? If yes, describe the MDM capabilities.	
S&D-58.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(2)	Is the institution capable of remotely wiping the mobile BYOD if it is lost or stolen?	
S&D-59.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(2)	Are portable devices disabled or automatically scanned for malware upon usage?	
S&D-60.EN	How are mobile devices returned to the institution when an employee leaves the institution, changes positions and/or upgrades equipment?	

SUPPORT & DELIVERY		
Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(2)		
S&D-61.EN Request List: IT-1 FTC Citation: 16 CFR 314.4(c)(1)	Are employees required to use only secured wireless connections both at work and when working remotely?	
S&D-62.EN Request List: Observe FTC Citation: 16 CFR 314.4(c)(1) 16 CFR 314.4(c)(8)	Is the physical environment actively monitored by cameras, badge reviews, etc.?	
S&D-63.EN Request List: IT-1, IT-12 FTC Citation: 16 CFR 314.4(c)(1) 16 CFR 314.4(c)(8)	What type of credentials are used to physically access institutional resources?	
S&D-64.EN Request List: IT-1, IT-12 FTC Citation: 16 CFR 314.4(c)(1) 16 CFR 314.4(c)(8)	What credentials are used to logically access resources?	

SUPPORT & DELIVERY		
S&D-65.EN Request List: Observe FTC Citation: 16 CFR 314.4(c)(1) 16 CFR 314.4(c)(8)	Are logs, including access logs, kept for the data center and/or other sensitive spaces?	
S&D-66.EN Request List: Observe	Is the location of computer equipment discrete?	
S&D-67 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.	
S&D-68 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?	

SUPPORT & DELIVERY		
S&D-69.EN Request List: Observe	Are business continuity and disaster recovery plans accessible in the event of an emergency?	
S&D-70 Request List: IT-11(e) FTC Citation: 16 CFR 314.4(d)(1)	Are business continuity and disaster recovery plans appropriately tested regularly?	
S&D-71 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?	
S&D-72.EN Request List: IT-11(e)	Do the test plans include varying scenarios including cyberattacks, internal interdependencies, documentation, analysis of results, use of offsite resources, critical third-party service providers, and remote access infrastructure and capacity?	
S&D-73.EN Request List: IT-11(e) Observe	Did the institution follow their business continuity and/or disaster recovery plans as written after testing or an actual incident?	
S&D-74 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?	
S&D-75 Request List: IT-11(b) FTC Citation: 16 CFR 314.4(c)(2)	Does the institution have a data backup program in place?	
S&D-76 Request List:	Is data backed up regularly and tested?	

SUPPORT & DELIVERY		
IT-11(b) FTC Citation: 16 CFR 314.4(c)(2) 16 CFR 314.4(d)(1)		
S&D-77 Request List: IT-11(b)	Is data stored offline to mitigate the risk of a ransomware attack on the online backup?	
S&D-78 Request List: IT-11(b)	Can the institution successfully restore information and resume business operations from backups? Indicate the date this was last tested.	
S&D-79.EN Request List: IT-11(b)	Are policies, procedures, and practices in place to allow the institution to restore its previous software versions in the event a software modification adversely affects one or more systems?	
S&D-80.EN Request List: Observe	Is there appropriate fire detection and containment equipment in the data center?	
S&D-81.EN Request List: Observe	Are there appropriate environmental controls in place in the data center so that the necessary humidity and temperature are maintained?	
S&D-82.EN Request List: Observe	Is the data center or other critical facility on an uninterruptable power supply (UPS) and generator that are tested regularly? Indicate the last date the UPS and generator were tested.	
S&D-83 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?	
S&D-84 Request List: IT-1, IT-10	Does the incident response plan address responsibilities and decision-making authorities for designated teams and/or staff members?	

[*] *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		
FTC Citation: 16 CFR 314.4(h) *		
S&D-85 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.	
S&D-86.EN Request List: IT-1, IT-10 FTC Citation: 16 CFR 314.4(h)	Do employees know who to contact in the event of an incident?	
S&D-87.EN Request List: IT-1, IT-10 FTC Citation: 16 CFR 314.4(h)	What reporting procedures are in place?	
S&D-88.EN Request List: IT-1, IT-10 FTC Citation: 16 CFR 314.4(c)(2))	Are there documented procedures in place for reporting lost or stolen mobile devices (e.g., phones, laptops, tablets USBs, CDs, removable hard drives, etc.)?	
S&D-89.EN Request List: IT-1, IT-10 FTC Citation: 16 CFR 314.4(h)	How are incidents communicated after resolution?	
S&D-90.EN Request List:	What internal stakeholders are notified?	

SUPPORT & DELIVERY		
IT-1, IT-10 FTC Citation: 16 CFR 314.4(h)		
S&D-91.EN Request List: IT-1, IT-10 FTC Citation: 16 CFR 314.4(h)	What external stakeholders are notified?	
S&D-92 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.	
S&D-93 Request List: IT-1, IT-10	Are event logs collected or stored in a centralized location for later review?	
S&D-94 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.