Nonbank Cybersecurity Exam Program Document Request List

Released Date: 05/09/2022
Version 1.0

Summary: This information technology (IT) and cybersecurity document request list was created by state regulators to assist in the examinations of nonbank institutions. The request list is to be used for the Baseline Nonbank Cybersecurity Exam Program (V1.0) and the Enhanced Nonbank Cybersecurity Exam Program (V1.0).

Ref. No.	Program Area	Requested Documents	Documents Provided	Institution Contact
IT – 1	Information Security Program	a) All policies and procedures that comprise the information security program, including but not limited to: • Information Security • Anti-virus • Change Management • Software Development and Maintenance • Vendor Management • Business Continuity/Disaster Recovery/Emergency Preparedness/Incident Response/Pandemic Plans • Remote Access for Employees and Customers • Data Backups • Data Retention • Data Disposal • Acceptable Use • Rules of Behavior • Clean Desk • Encryption/Data at Rest and Data in Motion • Mobile Device Management, including Bring Your Own Device • Written hardware and software end-of-life policies and procedures b) Risk Assessment(s) c) Information Security training materials for all employees, including employee completion records		
IT – 2	Board/ Management Oversight	a) IT Strategic Plan/Budget b) Most recent CIO or CISO presentation c) Materials to support Board discussion of risk acceptance d) Board/committee minutes to support designation of employee(s) to coordinate the information security program		
IT – 3	IT/IS Organization	a) IT/IS Organizational Chart(s) b) Resumes for key IT personnel c) Job descriptions for key IT personnel d) IT Succession Plan (if separate from overall institution plan)		
IT – 4	Relationships Between Assets and Data Flow	a) Network Diagram(s) b) Data Flow Diagram(s) c) Inventory of approved hardware and software assets, including network monitoring tools		

Ref. No.	Program Area	Requested Documents	Documents Provided	Institution Contact
IT – 5	Vulnerability Management Program	a) Written policies and procedures, if not already provided for #1 above b) Vulnerability scans – most recent c) Penetration tests/vulnerability assessments – most recent d) Remediation Actions		
IT – 6	Patch Management Program	a) Written policies and procedures, if not already provided for #1 above b) Patch deployment confirmation		
IT – 7	Change Management Program (includes software development activities)	a) Written policies and procedures, if not already provided for #1 above b) List of software development, acquisition, and maintenance changes within past 12 months c) List of hardware acquisition and maintenance changes within past 12 months		
IT – 8	IT Audit Function	a) IT Audit Policy b) Current and previous IT audit schedule c) IT audit risk assessment and audit plan d) IT audit reports for the past 24 months, including the corresponding engagement letters, if applicable e) Actions taken to remediate findings f) IT audit and regulatory finding tracking list g) Audit Organizational Chart		
IT – 9	Vendor Management Program	a) Written policies and procedures, if not already provided for #1 above b) List of third-party vendors, indicating which vendors are considered critical c) Documentation supporting compliance with vendor management program such as audit reports, contracts, due diligence, financial statement reviews, etc. (a sample will be selected upon receipt of the third-party vendor list)		
IT – 10	Incident Response	a) Incident Response Plan, if not already provided for #1 above b) Documentation to support most recent incident response plan test, including any remediation plans c) List of incidents occurring within previous 12 months		

Ref. No.	Program Area	Requested Documents	Documents Provided	Institution Contact
IT – 11	Business Continuity/ Disaster Recovery/ Emergency Management	a) Business Continuity/Disaster Recovery/ Emergency Management/Pandemic Plans, if not already provided for #1 above b) Backup policies and procedures, if not already provided for #1 above c) Business Impact Analysis d) Risk Assessment e) Documentation to support all testing performed during previous 24 months, including any remediation plans		
IT – 12	Password Management	a) Password settings for all systems b) Screen lockout settings for all systems c) Session expiration settings for all systems		
IT – 13	Remote Access for Employees and Customers	a) Written policies and procedures, if not already provided for #1 above b) Description of who all has remote access, including third-parties, employees and board members with company-owned devices and employees and board members with personal devices		
IT – 14	Insurance policies (*if applicable*)	a) Cybersecurity, ransomware, data breach notification b) Description of cyber insurance policy rejections, if any c) Description of payouts related to a cyber insurance policy over the past 24 months		
IT – 15	Products and Services	Describe the technology environment: a) Describe all cloud services used by the institution. Include Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). b) List of all core applications, including online applications and network(s), and indicate whether the applications are outsourced or hosted in-house. • If outsourced, please provide the name and location of the third-party provider. • If in-house, please indicate whether the applications are developed and maintained in-house or are a third-party software product. • Include the product name and third-party provider name and location for software products. c) Describe processes for network monitoring (e.g., performance, intrusion detection, web filtering) and network operations. Include whether these activities are outsourced or performed in house.		

State Specific Documents

Ref. No.	Program Area	Requested Documents	Documents Provided	Institution Contact
IT – 16				
IT – 17				
IT – 18				
IT – 19				
IT – 20				