Baseline Declarative Statements for Evaluation

Domain 1: Risk Management: Risk Assessment: The risk assessment is updated to address new technologies, products, services, and connections before deployment. (FFIEC Information Security Booklet, page 13)

Domain 3: Preventative Controls: Infrastructure Management: All ports are monitored. (FFIEC Information Security Booklet, page 50)

Domain 3: Preventative Controls: Infrastructure Management: Ports, functions, protocols and services are prohibited if no longer needed for business purposes. (FFIEC Information Security Booklet, page 50)

Domain 3: Preventative Controls: Infrastructure Management: Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. (FFIEC Information Security Booklet, page 56)

Domain 3: Preventative Controls: Access and Data Management: All default passwords and unnecessary default accounts are changed before system implementation. (FFIEC Information Security Booklet, page 61)

Domain 3: Preventative Controls: Access and Data Management: All passwords are encrypted in storage and in transit. (FFIEC Information Security Booklet, page 21)

Domain 3: Preventative Controls: Access and Data Management: Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. (FFIEC Information Security Booklet, page 45)

Domain 3: Detective Controls: Threat and Vulnerability Detection: Firewall rules are audited or verified at least quarterly. (FFIEC Information Security Booklet, page 82)

Domain 3: Detective Controls: Anomalous Activity Detection: The institution is able to detect anomalous activities through monitoring across the environment. (FFIEC Information Security Booklet, page 32)

Domain 3: Detective Controls: Anomalous Activity Detection: Access to critical systems by third parties is monitored for unauthorized or unusual activity. (FFIEC Outsourcing Booklet, page 26)

Domain 3: Detective Controls: Event Detection: A normal network activity baseline is established. (FFIEC Information Security Booklet, page 77)

Domain 3: Detective Controls: Event Detection: Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. (FFIEC Information Security Work Program, Objective II: M-9)

Domain 3: Corrective Controls: Patch Management: Patches are tested before being applied to systems and/or software. (FFIEC Operations Booklet, page 22)

Domain 4: Connections: Connections: Data flow diagrams are in place and document information flow to external parties. (FFIEC Information Security Booklet, page 10)

Domain 5: Incident Resilience Planning and Strategy: Testing: Scenarios are used to improve incident detection and response. (FFIEC Information Security Booklet, page 71)