BUSINESS ONLINE BANKING SERVICES

RISK ASSESSMENT AND CONTROLS EVALUATION CHECKLIST

DATE:

BUSINESS NAME:

ONLINE BANKING USER FIRST AND LAST NAME:

Review the security control recommendations listed below and place a check beside those that apply to your business environment. The purpose of this exercise is to evaluate your security posture and determine gaps. Consider which controls you have not checked that would be beneficial in mitigating risks.

Administrative Controls

- ☐ Management understands responsibilities and liabilities per the financial institution's account agreement
- ☐ Employees are educated on use of application(s), IT security standards and best practices, common fraud schemes and procedures for contacting the FI in case of suspected security incident
- ☐ Employees are on the alert for rogue emails
- ☐ Employees have segregation of duties, a separate approval process and dual control utilizing two separate PCs for online transactions
- ☐ Employees close out of the browser session of their online banking session as soon as they are finished
- ☐ Strong passwords are in use with 8-10 characters that use a combination of upper and lower case letters along with numbers and special characters
- ☐ The default password on all network devices has been changed
- ☐ Online banking passwords are not shared with anyone
- ☐ The same passwords are not used to access different systems
- ☐ Passwords are changed every 60-90 days
- ☐ Accounts are monitored and reconciled daily

Administrative Controls cont.

- [ ] Public computers are not used to conduct online banking transactions
- [ ] Each online banking session is confirmed to begin with *https* instead of *http* indicating a secure browser setting
- [ ] The internet browser's cache is cleared before starting an online banking session
- [ ] The PC used for online banking is not used to surf the web or email

Technical Controls

- [ ] Real-time anti-virus and anti-spyware, desktop firewall, malware detection and removal software w/automatic updates and scheduled scans are installed
- [ ] Installed ant-virus, anti-spyware and malware software is from a professional resource. Free software is not robust enough
- [ ] Implement a dedicated firewall and router that are actively managed
- [ ] Options offered by the FI to detect or prevent out-of-pattern activity have been discussed
- [ ] Changes in the online banking PC's performance are investigated that signify a machine has been compromised
- [ ] A vulnerability assessment from a security expert has been considered or executed to determine any potential security issues
- [ ] Internet browser are set to block all pop ups
- [ ] User rights for online banking computers are limited. For example, administrative rights are restricted so that not every user can download software onto the computer
- [ ] Security patches are up to date for operating system and other software applications

Physical Controls

- [ ] Computers are never unattended while logged into an online banking session
- [ ] The online banking computer is shut down and/or disconnected from the internet when not in use for significant time periods
- [ ] Remembrance features are avoided such as writing down user name and password

EVALUATION NOTES: