COMMERCIAL RISK ASSESSMENT AND CONTROLS EVALUATION

Date Conducted: **Conducted By:**

PURPOSE

The following risk assessment and controls evaluation is provided to assist commercial Internet banking users in identifying threats and measure the strength of their controls.

RISK ASSESSMENT

For each question, select the answer(s) that best represent(s) your environment. Following the assessment, use the “Control Evaluation - Best Answers and Tips” to evaluate your environment.

Personnel Security:

1) Are all employees required to sign an Acceptable Use Policy (AUP)?
   a) Yes, at least annually or more frequently as needed (1)
   b) Yes, but only at hire (2)
   c) No (5)

2) Does each employee go through Information Security training?
   a) Yes, at least annually or more frequently as needed (1)
   b) Yes, but only at hire (2)
   c) No (5)

3) Are background checks run on employees prior to hire?
   a) Yes, for all employees (1)
   b) Yes, but only based on position (2)
   c) No (5)

Computer Network Security:

4) Do computer systems have up-to-date antivirus software?
   a) Yes, all systems (1)
   b) Yes, but only critical systems (3)
   c) No (5)

5) Is there a process in place to ensure software updates and patches are applied (e.g. Microsoft, web browser, Adobe products, etc.)?
   a) Yes, a formal process where updates are applied at least monthly (1)
   b) Yes, but informally as needed (3)
   c) No (5)

6) Do users run as local Administrators on their computers?
   a) No (1)
   b) Only those that require it (3)
   c) Yes (5)

7) Is a firewall in place to protect the network? (This does not include windows firewall on local PC)?
   a) Yes (1)
   b) No (15)

8) Do you have an Intrusion Detection System (IDS) in place to monitor and protect the network?
   a) Yes (1)
   b) No (3)

9) Are you restricting Internet usage?
   a) Yes, Internet traffic is restricted - Restricting internet to only sites specifically needed for business functions (1)
   b) Yes, we have Internet content filtering (2)
   c) No (5)

10) Does e-mail have SPAM filtering?
   a) Yes (1)
   b) No (5)

11) Are users trained to manually lock their workstations when they are not present?
   a) Yes, and the systems are set to an automatic timeout after a period of inactivity (1)
   b) Yes, but it is only manually (2)
   c) No (5)

12) Is wireless technology used on the network?
   a) No (1)
   b) Yes, but wireless traffic uses industry-approved encryption (e.g. WPA, etc.) (1)
   c) Yes, but wireless uses WEP encryption (2)
   d) Yes, and wireless traffic is not encrypted (15)

Physical Security:

13) Are critical systems located in secure areas?
   a) Yes, behind a locked door (1)
   b) Yes, in a restricted area (2)
   c) No, in a public area (5)

14) How are passwords protected?
   a) Passwords are securely stored. (1)
   b) Passwords are written on paper or sticky notes and placed by the computer. (15)

Determining your Risk Rating

Once you have completed the questionnaire, add up the totals following the answers to determine your risk rating. Note: risk rating is intended to give a general idea of your risk position based only on the answers in this questionnaire. Additional factors will either increase or decrease the risk.

Risk Rating	
0-15	LOW
16-25	MEDIUM
26-35	HIGH
Over 35	EXTREME

Control Evaluation – Best Answers and Tips

Below are the results from the risk assessment. Review your answers and the tips to help you protect your systems and information.

1. The best answer is "Yes, at least annually or more frequent as needed." An Acceptable Use Policy (AUP) details the permitted user activities and consequences of noncompliance. Examples of elements included in an AUP are: purpose and scope of network activity; devices that can be used to access the network, permitted websites, password usage, circumventing controls or disrupting services; expected user behavior, and consequences of noncompliance.

2. The best answer is "Yes, at least annually or more frequently as needed." Information Secuirty Training at a minimum, should include a review of the acceptable use policy, desktop security, log-on requirements, password administration guidelines, social engineering tactics, etc.

3. The best answer is "Yes, for all employees." Companies should have a process to verify job application information on all new employees. The sensitivity of a particular position or job junction may warrant additional background and credit checks. After employment, companies should remain alert to changes in employees' circumstances that could increase incentives for abuse or fraud. May be necessary to run continued background checks for long tenured employees.

4. The best answer is "Yes, all systems." Companies should maintain active and up-to-date antivirus/anti malware protection provided by a reputable vendor. Schedule regular scans of your computer in addition to real-time scanning.

5. The best answer is "Yes, a formal process where updates are applied at least monthly." Update your software frequently to ensure you have the latest security patches. This includes a computer's operating system and other installed software (e.g. web browsers, Adobe Flash Player, Adobe Reader, Java, Microsoft Office, etc.). In many cases, it is best to automate software updates when the software supports and can monitor updates.

6. The best answer is "No." Limit local Administrator privileges on computer systems when possible.

7. The best answer is "Yes." Use firewalls on your local network to add another layer of protection for all the devices that connect through the firewall (e.g. PCs, smart phones, and tablets).

8. The best answer is "Yes." Intrusion Detection Systems (IDS) are used to monitor network/Internet traffic and report or respond to potential attacks. Monitoring services monitoring the firewall are preferred.

9. The best answer is "Yes, Internet traffic is restricted - Restricting internet to only sites specifically needed for business functions." Filter Internnet Usage to restrict potentially harmful or unwanted Internet sites from being accessed by computer systems. For "high risk" systems, it is best to limit Internet sites to only those business sites that are required.

10. The best answer is “Yes.” Implementing e-mail SPAM filtering will help eliminate potentially harmful or unwanted e-mails from making it to end users’ inboxes.

11. The best answer is “Yes, and the systems are set with automatic timeouts after a period of inactivity.” Systems should be locked with automatic timeouts (requiring a password to reconnect) when users walk away from their computers to prevent unauthorized access to the system.

12. The best answers are either “No” or “Yes, but wireless traffic uses industry approved encryption (e.g. WPA, etc.).” Wireless networks are considered public networks because they use radio waves to communicate. Radio waves are not confined to specific areas and are easily intercepted by unauthorized individuals. Therefore, if wireless is used, security controls such as encryption, authentication, and segregation are necessary to ensure confidentiality and integrity.

13. The best answer is “Yes, behind a locked door.” Critical systems should be secured to only allow access to approved employees. It is even sometimes nessary to put devices under dual control.

14. The best answer is “Passwords are securely stored.” Passwords should remain private. Employees should never share passwords.

Contacts

In the event of suspicious activity or if you believe your account information is at risk, please contact us.

To report issue regarding online banking or ACH services please contact 405-715-1100.

To report a lost of stolen debit card, please call 405-348-1500. After hours please call 1-800-523-4175

If you have any questions you may email us at helpdesk@fmbankok.com (please do not include confidential information via this unsecure email)