Commercial Risk Assessment and Controls Evaluation

Date Conducted: _____ **Conducted By:** _____

Purpose

The following e-banking 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 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 using Internet banking complete security awareness training?
   a) Yes, at least annually or more frequently as needed (1)
   b) Yes, but only at hire (2)
   c) No (5)

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

Computer System Security:

4) Is a dedicated computer system used for e-Banking activities?
   a) Yes, the system is dedicated to only e-Banking activities (1)
   b) No, the system is used for other business purposes (5)

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

6) Is there a process in place to ensure software updates and patches are applied (e.g. Microsoft, Java, 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)

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

8) Does a firewall protect the network?
   a) Yes (1)
   b) No (15)

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

10) Is Internet content filtering being used?
   a) Yes, Internet traffic on the system used for “high risk” Internet banking activities is restricted to only those sites specifically needed for business functions (1)
   b) Yes, we have Internet content filtering (2)
   c) No (5)

11) Is email SPAM filtering being used?
   a) Yes (1)
   b) No (5)

12) Are users of the Internet banking system trained to manually lock their workstations when they leave them?
   a) Yes, and the systems are set to auto-lock after a period of inactivity (1)
   b) Yes, but auto-lock is not enabled (2)
   c) No (5)

13) Is wireless technology used on the network with the Internet banking system?
   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:

14) Are critical systems (including systems used to access Internet banking) located in a secure area?
   a) Yes, behind a locked door (1)
   b) Yes, in a restricted area (2)
   c) No, in a public area (5)

15) 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)

Previous Experience:

16) Have you experienced fraud through e-Banking in the past?
   a) No (1)
   b) Yes, attempted fraud, but it was detected and stopped (3)
   c) Yes (5)

17) Has malware been discovered on systems used for e-Banking activities in the past?
   a) No (1)
   b) Yes (5)

Risk Rating

Once you have completed the questionnaire, total the answers selected to calculate a summary risk rating of your environment. Note: This risk rating is designed to give a general idea of your risk posture based only on the answers in this questionnaire. Additional factors could either increase or decrease the risk.

Overall Risk Rating	
0-20	LOW
21-30	MEDIUM
31-40	HIGH
Over 40	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 "a) 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, bans on attempting to break into accounts, crack passwords, circumvent controls or disrupt services; expected user behavior; and consequences of noncompliance.

2. The best answer is "a) Yes, at least annually or more frequently as needed." Security Awareness Training (SAT) for Internet banking users should include, at a minimum, a review of the acceptable use policy, desktop security, log-on requirements, password administration guidelines, social engineering tactics, etc.

3. The best answer is "a) 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 function 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.

4. The best answer is "a) Yes, the system is dedicated to only e-Banking activities." It is best to have a dedicated system for high-risk e-Banking activities.

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

6. The best answer is "a) 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.). It is best to automate software updates when the software supports it.

7. The best answer is "a) No." Limit local Administrator privilege on computer systems where possible.

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

9. The best answer is "a) Yes." Intrusion Detection/Prevention Systems (IDS/IPS) are used to monitor network/Internet traffic and report or respond to potential attacks.

10. The best answer is “a) Yes, Internet traffic on the system used for “high risk” Internet Banking activities is restricted to only those sites specifically needed for business functions.” Filter web traffic 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.

11. The best answer is “a) Yes.” Implementing email SPAM filtering will help eliminate potentially harmful or unwanted emails from being delivered to end users’ inboxes.

12. The best answer is “a) Yes, and the systems are set to auto-lock after a period of inactivity.” Systems should be locked (requiring a password to reconnect) when users walk away from their desks to prevent unauthorized access to the system.

13. The best answers are either “a) No” or “b) 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.

14. The best answer is “a) Yes, behind a locked door.” Physically secure critical systems to only allow access to approved employees.

15. The best answer is “a) Passwords are securely stored.” Passwords should never be exposed to unauthorized individuals.

16. The best answer is “a) No.”

17. The best answer is “a) No.” If you have discovered malware on the e-Banking system in the past, ensure the system is clean of all malware. It is best to do this by rebuilding the system.