The following Business eBanking Risk Assessment and Controls Evaluation is provided to help you, as a principal or business owner, identify threats to your company's commercial Online Banking practices and to provide best practices to ensure necessary controls are in place.

For each question, select the answer that best represents your environment. You'll see a number listed after each possible answer. These numbers will be used to calculate a risk score.

At the end of the assessment, you'll notice a section called "Best Answers & Tips." Use this to evaluate your environment and to make any necessary changes. This risk assessment and the tips provided, should be adapted to fit your company's technology capabilities and specific needs.

RISK ASSESSMENT

Computer System Security

1. Do computer systems have up-to-date antivirus software?
    a. No (5)
    b. Yes, all systems (1)
    c. Yes, but only critical systems (2)
2. Is there a regular process in place to apply software updates and patches (e.g. Microsoft, web browser, Adobe products, etc.)?
    a. No (5)
    b. Yes, a formal process where updates are applied at least monthly (1)
    c. Yes, but only when time permits (3)
3. Do employees have Local Administrator (Admin) privileges on their PCs or laptops?
    a. No (1)
    b. Only those that require it (3)
    c. Yes (5)
4. Is a firewall in place to protect the network?
    a. No (15)
    b. Yes (1)
5. Do you have an Intrusion Detection/Prevention System (IDS/IPS) in place to monitor and protect the network?
    a. Yes (1)
    b. No (3)
6. Is Internet content filtering being used?
    a. No (5)
    b. Yes, Internet traffic on the system used for "high risk" Internet banking activities is completely restricted to only sites specifically needed for business functions (1)
    c. Yes, we have Internet content filtering (2)
7. Is email SPAM filtering being used?
    a. No (5)
    b. Yes (1)
8. Are users of the Internet banking system trained to manually lock their work stations when they leave them?
    a. No (5)
    b. Yes, but it is only manually (2)
    c. Yes, and the systems are set to auto-lock after a period of inactivity (1)

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

Physical Security

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

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

Personnel Security

12. Are employees required to sign an Acceptable Use Policy (AUP)?
    a. No (5)
    b. Yes, at least annually (1)
    c. Yes, but only one time during the new-hire process (2)

13. Does each employee using Online banking complete security awareness training?
    a. No (5)
    b. Yes, but only at hire (2)
    c. Yes, at least annually or more frequently as needed (1)

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

15. Do you periodically review User's access to sensitive systems such as Mobile Banking or Online Banking access?
    a. No (10)
    b. Yes, for all systems annually (5)
    c. Yes, quarterly certifications to payment systems are conducted (1)

RISK RATING

Once you have completed the questionnaire, add up the numbers next to each answer you have selected above. Using your total, note where you fall on the Overall Risk Rating chart.

Overall Risk Rating	
0 - 17	Low
18 - 26	Medium
27 - 38	High
Over 38	Extreme

Compare your answers to the Business eBanking Risk Assessment to the "Best Answers" below. Tips are also provided to help you protect your systems and information.

CONTROL EVALUATION – Best Answers & Tips

1. The best answer is **b)** Companies should maintain active and up-to-date antivirus protection provided by a reputable vendor. Schedule regular scans of your computer in addition to realtime scanning.
2. The best answer is **b)** 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 it.
3. The best answer is **a)** Limit local Administrator privilege on computer systems where possible.
4. The best answer is **b)** 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).
5. The best answer is **a)** Intrusion Detection/Prevention Systems (IDS/IPS) are used to monitor network/Internet traffic and report or respond to potential attacks.
6. The best answer is **b)** 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.
7. The best answer is **b)** Implement email SPAM filtering to help eliminate potentially harmful emails from making it to end users' inbox.
8. The best answer is **c)** Systems should be automatically locked (requiring a password to reconnect) when users walk away from their desks to prevent unauthorized access to the system.
9. The best answers are either **a)** or **c)** Wireless networks are considered public networks because they use radio waves to communicate. Radio waves 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.
10. The best answer is **c)** Physically secure critical systems to only allow access to approved employees.
11. The best answer is **a)** Passwords should never be left out for unauthorized individuals to gain access. Assign someone to walk around periodically and check under keyboards, post-it notes around monitors or desktops to make sure that employees maintain passwords securely.
12. The best answer is **b)** 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; and expected user behavior.
13. The best answer is **c)** Security Awareness Training (SAT) for Online banking users, at a minimum, should include a review of the acceptable use policy, desktop security, log-on requirements, password administration guidelines, social engineering tactics, etc.
14. The best answer is **b)** 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.
15. The best answer is **c)** Employees may be able to access bank accounts using Online banking services long after they have left the company, unless periodic access reviews are conducted. Make sure to terminate access immediately for employees who have left the company, as well as those who take a leave of absence and check access to sensitive systems at least quarterly to catch any oversight.

RESOURCES

Your online safety and financial health are very important to us. For more information and resources regarding online security, please visit pbofca.com.

If you have any questions or need assistance regarding business ebanking or any of our products and services, please give us a call at (866) 323-2741 or email us at onlinebanking@pbofca.com.