BankersOnline.com

Checklist for Information Security Steps

Access Controls and User Permissions

Have you employed effective access controls to restrict access to computer programs and data and prevent and detect unauthorized access?

____ Do employees have the authority to only read or modify those programs and data that they need to perform their duties?

____ Do outside contractors have the authority to only read or modify those programs and data that they need to perform their duties?

____ Do you have a workable procedure for assigning user access rights and permissions?

____ Have you established a process for reviewing the appropriateness of individual access privileges?

____ Does your process include a comprehensive method for identifying and reviewing all access rights granted to any one user?

____ Do you frequently/periodically review access rights and permissions to ensure that access remains appropriate on the basis of job responsibilities?

___ Does your user access scheme guard against heightened vulnerability that can result from users that are system developers who may have detailed knowledge of the systems' processing functions that could allow them to improperly add, alter, or delete critical financial and sensitive information or programs, possibly without detection?

____ Have you adequately restricted users from viewing sensitive information?

Network Security

_____ Are you staying informed about software vulnerabilities and securing your network against them by addressing them in an appropriate and timely fashion?

_____ Have you restricted access to sensitive network resources in order to reduce the chance that someone with access could obtain copies or modify configuration files containing control information, such as access control lists, and disable or disrupt network operations by controlling critical or sensitive network resources?

_____ Have you adequately restricted access connectivity to critical network resources?

_____ Are you controlling network connections to/from off-site locations?

_____ Do you have a process for assessing third-party contractor connectivity requirements?

_____ Do you routinely review user access activity?

_____ Do you routinely investigate failed attempts to access sensitive data and resources?

_____ Do you routinely investigate unusual and suspicious patterns of successful access to sensitive data and resources?

_____ Do you maintain logs of user activity for all critical processing activities?

_____ Do you collect and monitor activities on all critical systems, including mainframes, network servers, and routers?

____ Do you have an actual monitoring strategy for information technology security that includes monitoring, event correlations, and incident identification and response?

_____ Do you utilize an intrusion detection system (IDS) that monitors all key network resources and automatically logs unusual activity, provides necessary alerts, and terminates access?

____ Are the duties and responsibilities of staff assigned to the monitoring program adequately segregated to ensure a system of checks and balances in order to guard against alteration?

____ Do you have adequate staff to allow you to segregate responsibilities in this area?

Computer Security Program

_____ Are your information security policies and procedures:

- based on risk assessments;
- designed to cost effectively reduce risks;
- designed to ensure that information security is addressed throughout the life cycle of each system;
- designed to ensure compliance with applicable requirements?

_____ Do you provide security awareness training to inform personnel, including contractors and other users of information systems, about information security risks and your own procedures and their responsibilities for complying with your policies and procedures?

_____ Do you perform periodic assessments of the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems and make changes to your policies and procedures as the risks warrant?

_____ Do you have a framework for assessing and managing risks on a continuing basis that specifies:

- how the assessments should be initiated and conducted;
- who should participate in the assessment;
- how disagreements should be resolved;
- what approvals are needed; and
- how the assessments should be documented and maintained?

_____ Do you periodically test and evaluate the effectiveness of information security policies, procedures, and practices with a frequency that depends upon risk, but no less than annually, that includes testing of management, operational, and technical controls of major information systems?

_____ Do you have proper accountability and authority for your information security management function?

_____ Do you have a policy on network password standards, and do you require adherence to it?

_____ Do you provide more specialized security awareness training for selected technical staff?

_____ Do you keep records of the security awareness training of ALL staff?

_____ Does your testing and evaluation procedure include ongoing reviews, tests, and evaluations of information security to ensure your systems are in compliance with policies and procedures and to identify and correct weaknesses?

_____ If you rely upon contractors to support your systems and you provide them with connections and access to your internal network, have you performed an appropriate security review of these contractor connections?

_____ Do you have an ongoing process to collectively analyze related weaknesses for systemic problems that could adversely affect critical systems?

_____ Are corrective actions documented, tracked, and independently tested or reviewed for appropriateness and effectiveness?

Author, Mary Beth Guard. (This checklist is based upon data extracted from GAO-04-630.) This checklist appears on Banker Tools on BankersOnline.com. www.bankersonline.com/tools/tools.html