



April 2004

IN THIS ISSUE

2
Common
Weaknesses

2
Common
Strengths

Preparing for Your Bank's IT Exam – Part 2

By: Cynthia A. Bonnette, Director of Information Security Risk Assessment, NETBankAudit

Preparing for the IT Exam

Part 1 of this article highlighted a number of changes that have occurred in the IT examination process. In particular, the six new IT Booklets issued by the FFIEC have introduced additional requirements that may take many bankers by surprise. To best prepare for your next IT exam and minimize the likelihood of unpleasant surprises, this article offers some specific recommendations. ■

Pitfalls and Successes

Common Weaknesses

- Exclusive focus on technical issues (lack of attention to strategy and administration).
- Lack of documented board involvement.
- Undefined responsibility for information security.
- Lack of comprehensive and documented risk assessments.
- Lack of uniform controls (inconsistent practices).
- Lack of skilled staff (failure to train, inadequate depth).
- Weak or non-existent policies and procedures.
- General lack of documentation (e.g., logs and monitoring reports).
- Failure to coordinate, prioritize, and follow-up on test results.

Preparing for an examination can be a bit like Russian roulette—there is a lot of uncertainty involved, and how you spend your time and resources might pay off well or result in unexpected problems. For example, documenting your strategies, risk management decisions, policies, and practices is essential. However, over-documenting can lead to confusion, conflicts, and

unnecessary critiques. Striking the proper balance can be more of an art than a science.

The new FFIEC Booklets, along with examination workprograms issued by individual regulators (e.g., FDIC's IT-MERIT and IT General Workprogram) outline the rules of the road. However, the depth and scope of the examination will also depend on your bank's prior history with the regulators, the quality of documentation and processes, and the examiners' expertise. Proper preparation can go a long way toward improving your chances of a successful IT examination, and ten steps are recommended below:

1. Know the Rules

It's essential to stay abreast of the standards against which you will be measured and therefore you need to keep up with current guidance and regulations (e.g., the new FFIEC Booklets). Awareness of best practices and rules that may not directly affect your bank (e.g., Sarbanes Oxley Section 404, which addresses internal controls) is also recommended.

2. Address Criticisms from Past Exams

Common Strengths

- The board and senior management's involvement is active and documented.
- Formal designation of responsibility for information security.
- Formation of a cross-department working group for strategic issues (e.g., information security, business continuity).
- Formalized risk assessment process.
- Formalized policies and procedures.
- Centralized controls for the entire organization.
- Effective, coordinated testing processes.
- Periodic self-assessments using regulatory exam procedures.
- Periodic staff training.

Nothing upsets bank examiners more than open criticisms from prior exams. Even if the items were disputed, leaving them unaddressed will never be in your best interests. Documentation of your plans to address these items is far better than ignoring them.

continued on page 2



PITTFALLS AND SUCCESSES continued from page 1

3. Document Testing and Monitoring Processes

Examiners like documentation, and even more, they like documentation that provides a clear audit trail. Logs and management reports will be reviewed to confirm that you are recording significant events and following up. Your documentation should demonstrate that you are tracking the right things and that the logs and other reports are actively reviewed.

4. Document Management and Board Oversight

Oversight by management and the board is specifically required by the Safeguarding Customer Information Standards and the FFIEC Booklets. However, equally important is that this involvement be documented. Some banks have been criticized because they were unable to show that directors had received and discussed updates on information security. Be sure that your board minutes and supporting materials provide this evidence.

5. Document Plans for Completing Work-in-Process

Examiners understand that information security and general IT operations are ongoing processes. They are often satisfied with the knowledge that your bank has identified what needs to be done and working toward accomplishing it. Therefore, when you identify gaps that may not be addressed in time for the exam, a plan for completing the project will serve you well. You may also benefit from examiner feedback on your plan, which will help to ensure that the final product will meet with approval.

6. Conduct Exam Procedure Walk-Throughs

It is always better to find your own mistakes or omissions than to leave them for identification by examiners. By conducting a walk-through of the examination procedures contained in the FFIEC Booklets and other exam procedures, you will know clearly where you stand. It is best to complete this exercise well in advance of the scheduled exam to provide sufficient time for corrective action.

7. Conduct and Follow-up on Internal and External Tests

Examiners love to follow other examiners' and auditors' work. Generally, the first items on their request list are the prior examination and audit reports. Be sure that you have documented the status of all open items from recent reviews. You should also have a documented information security testing plan that meets the guidelines in the *FFIEC Information Security Booklet*.

8. Ensure that Policies and Procedures are Realistic

It is never a successful practice to create policies that you can't live with, even if they are written to meet the stated regulatory requirements. Ultimately, you will end up in non-compliance and a clear target for criticism. A better plan is to modify your policies to better suit your situation and provide for an exceptions process to address unforeseen circumstances.

9. Communicate with Peer Banks about their Experiences

Comparing notes with other bankers can be a good way to avoid surprises. While the respective regulatory agencies still have their differences in style and approach, the IT exam is probably the area of greatest consistency. Patterns such as heightened scrutiny of information security programs, IT audit, and business continuity plans are presently being observed across the board.

10. Stay in Touch with your Regulators

An open communication channel with your examiners and regional or district office representative is another valuable resource. As you respond to prior examination criticisms or develop new procedures in response to the FFIEC guidance, it can be helpful to confirm your progress.

Preparing for your next IT exam can be a challenging process that requires advance planning and sufficient time to complete a self-assessment and address what you find. By keeping current with regulatory requirements on an ongoing basis and periodically updating your documentation, you can avoid having to play "catch-up" at crunch time. ■

NETBankAudit specializes in information security and technology risk assessment services with a focus on high quality, low maintenance, cost effective solutions that help financial institutions meet regulatory requirements and industry best practices. Founded in 2000, NETBankAudit offers financial institutions the ability to audit and test their network security architecture, policy and procedures, and regulatory compliance. Visit www.netbankaudit.com for further information.

Common Weaknesses

- Exclusive focus on technical issues (lack of attention to strategy and administration).
- Lack of documented board involvement.
- Undefined responsibility for information security.
- Lack of comprehensive and documented risk assessments.
- Lack of uniform controls (inconsistent practices).
- Lack of skilled staff (failure to train, inadequate depth).
- Weak or non-existent policies and procedures.
- General lack of documentation (e.g., logs and monitoring reports).
- Failure to coordinate, prioritize, and follow-up on test results.

Common Strengths

- The board and senior management's involvement is active and documented.
- Formal designation of responsibility for information security.
- Formation of a cross-department working group for strategic issues (e.g., information security, business continuity).
- Formalized risk assessment process.
- Formalized policies and procedures.
- Centralized controls for the entire organization.
- Effective, coordinated testing processes.
- Periodic self-assessments using regulatory exam procedures.
- Periodic staff training.

