



NON-GEEK SPEAK

A Technology Newsletter for the CEO



March 2004

IN THIS ISSUE

- 2 Other Important Developments
- 2 Preparing for the IT Exam
- 2 Essential Resources

Preparing for Your Bank's IT Exam

A Wake-Up Call

The examiners have arrived and they are asking to review your information security testing plan and risk assessment documentation. They would also like a copy of the business impact analysis and risk assessment supporting your business continuity plan. In addition, they are requesting the bank's electronic banking strategy and policy. At this point, many bankers experience shock and frustration. What are all these new requirements and when did the rules of the game change? ■

FFIEC Information Technology Handbook (Booklets)

Information Security

Issued in December 2002, this booklet provides guidance on what examiners expect in an information security program. Certain items that may be new to bankers include the following:

- Information Security Risk Assessment
- Information Security Testing Plan
- Logging and Data Collection
- Intrusion Detection and Incident Response

Tip: Each section of the booklet begins with an "Action Summary" that highlights key points. This should be your checklist for ensuring that you are prepared for the next exam.

Business Continuity Planning

A significant characteristic of the BCP Booklet is the change from "Disaster Recovery" to "Business Continuity." This reflects a new focus on the plan's scalability and coverage of a wide range of potential disruptions—not just a complete disaster scenario.

Changes in the IT Exam

The IT exam has been completely transformed over recent years. Even the name has changed from Electronic Data Processing, to Information Systems, and now Information Technology. Most importantly, changes have occurred in how the regulators view technology in the overall context of bank safety and soundness. In the past, "EDP" was generally considered a low risk area and tended to receive a cursory review at best. The turning point came with the dual events of Internet banking and Y2K. Regulators began to take notice and information technology became another area requiring risk management and controls.

The most significant development occurred with the enactment of the Gramm-Leach-Bliley Act and the Standards for Safeguarding Customer Information. Previously, information systems issues were treated as general safety and soundness matters and criticisms were addressed in the evaluation of management, or the "M" in the CAMELS rating. Now, with a formal regulation requiring information security controls, violations and enforcement actions may occur.

To support the Standards, exam guidance and procedures became more rigorous. The first few years of this process (the Standards took effect in July 2001) were educational for both bankers and examiners as expectations became better defined. Now, with the issuance of six FFIEC Information Technology Booklets, bankers have more specific and helpful guidance, however, the bar has been raised for what needs to be done and documented.



New items include:

- Business Impact Analysis
- Risk Assessment for Business Continuity
- Testing Plan

Tip: As many banks have not revisited their Plans since Y2K, now is the time to consider a complete overhaul that will incorporate the above items. The Examination Workprogram provided in the Booklet provides a helpful guide.

IT Audit

The IT Audit Booklet provides guidance on governance, independence, and development/maintenance of a comprehensive audit program. Helpful items include:

- Requirements for an External Audit Engagement Letter
- Items to Consider in a Risk Scoring System

Tip: The Booklet offers provides little guidance on developing an appropriate scope for the IT Audit (although the Examination Procedures (Tier II) list general categories that should be addressed). Bankers need to ensure that the audit scope is consistent and comprehensive. The scope of the IT audit should also be reconciled with the bank's information security testing plan (described in the Information Security Booklet).

Electronic Banking and Fedline

The Electronic Banking and Fedline Booklets build on prior guidance in supervisory bulletins. Important items to note include:

- Definition of Electronic Banking
- Authentication Practices

Tip: Consider adopting a broad definition of E-banking that is consistent with the regulatory standard. This will facilitate consolidation and streamlining of various policies and procedures that address various e-delivery and e-payment systems.

A Booklet on Technology Service Providers was issued, which addresses how examiners will evaluate third party service providers and is not particularly relevant for bankers. In the near future, six more booklets are expected on: Outsourcing and Vendor Management, Development and Acquisition, IT Management, Operations, Retail Payment Systems, and Wholesale Payment Systems. ■

Other Important Developments

Outsourcing and Vendor Management

While the new Booklet has yet to be published, examiners looking closely at banks' outsourcing practices. Adherence to the FFIEC guidance from November 2000 is the baseline, and bankers are expected to take a risk-focused approach to vendor management. In addition to a written Outsourcing and Vendor Management policy and procedures, important elements include:

- Vendor Inventory or Tracking System
- Risk Rating Methodology

Documentation

In general, examiners are looking for more documentation. Policies, procedures, management reports, logs, checklists, and workpapers go a long way toward demonstrating that your bank has taken the necessary steps to implement sound practices and meet regulatory requirements. As a standard practice, you should document your plans and schedules for accomplishing any significant items that have not yet been addressed.

Preparing for the IT Exam

Clearly there are a lot of new things in the IT Exam process and a number of important items to address prior to your next examination. Where should you start and what are the priorities for exam preparation? Part 2 of this article will provide you with specific suggestions and tips for preparing for your next IT examination and offer a "Top Ten" checklist of things to do to get ready.

"The author, Cynthia A. Bonnette, is Director of Information Security Risk Assessment for NETBankAudit. Previously, she spent thirteen years at the FDIC as a bank examiner, IT specialist, and assistant director. 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."

Essential Resources:

FFIEC IT Handbook (Booklets): http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#tsp

OCC Electronic Banking Guidance:

<http://www.occ.treas.gov/netbank/ebguide.htm>

FDIC Information Technology References:

<http://www.fdic.gov/regulations/examinations/index.html#Ebank>

OTS Electronic Banking Guidance:

<http://www.ots.treas.gov/>

[sort1.cfm?DOC_CAT=32&catNumber=103&catParent=0](http://www.ots.treas.gov/sort1.cfm?DOC_CAT=32&catNumber=103&catParent=0)

Federal Reserve Supervisory Information (There is no specific page for IT or E-banking):

<http://www.federalreserve.gov/banknreg.htm>

