

## MEMORANDUM

To: Subscribers to *Information Security Audit for Banks*

From: Sheshunoff Information Services

Subject: Highlights

---

Enclosed is the most recent update to *Information Security Audit for Banks*. With the constant threat of data compromise and on-going regulatory oversight, information security officers must continuously monitor IT systems and security processes. To further assist you and your management team, this update includes the following:

- *Identity Theft Red Flags*. In a joint release the regulatory agencies issued requirements for implementing an Identity Theft Prevention Program and providing sample red flags to consider when implementing your monitoring program. Financial institutions are expected to have your programs in place and operational by November 1, 2008. See Chapter 6.
- *Risk Management*. Chapter 7 has been expanded to include a discussion on developing an integrated risk management framework so that IT systems can be integrated with other related systems. Combining data systems can help you align risk exposure calculations more closely with your institution's underlying risks.
- *Business Continuity*. It is critical to evaluate your recovery capabilities with respect to potential disasters. IT disruptions could cause severe financial loss and threaten your institution's survival. Chapter 13 has been expanded to include an in-depth discussion on business continuity and technology assessment.