

Sheshunoff™

Dear Valued Customer,

With the fall flu season upon us and news of swine flu spreading, banks must have a plan ready in case of a pandemic. If more than half your staff was unable to come to work, how will you provide services to customers? In this latest update to *Information Security for Banks: Operations, Technology, and Compliance*, Chapter 27 has been updated with new information regarding business continuity planning. Specifically, the following discussions have been included:

- *Continuity Guidance Circular 1*. In January 2009, The Department of Homeland Security, FEMA, in coordination with non-federal partners, developed Continuity Guidance Circular 1 (CGC 1), Continuity Guidance for Non-Federal Entities (States, Territories, Tribal, and Local Government Jurisdictions and Private Sector Organizations). The purpose of this guidance document is to provide direction for the development of continuity plans and programs for non-federal entities.
- *Federal Continuity Directives*. In February 2008, the Department of Homeland Security issued Federal Continuity Directives 1 and 2 to help federal executive branch organizations, state and local governments, and the private sector develop continuity plans. FCD 2 focuses on identifying mission essential functions.
- *Identification of single points of failure*. A single point of failure is defined as a single element, component, system, device, or person that is critical to providing a service. Availability is the aspect of continuity planning that is concerned with avoiding single points of failure. After identifying priorities, management must research and evaluate the most practical alternatives for IT processing in case of a disaster.
- *Telephone services recovery strategies*. Voice communications recovery strategies are especially difficult because of the technology of voice systems and the limited recovery options available. Most organizations are highly dependent on voice communications to provide essential services; therefore, backup alternatives should be evaluated and implemented. The most frequent point of failure in many voice communications systems is the communications line. A new section in Chapter 14 discusses various recovery strategies.
- *ISO standards*. The ISO/IEC 27000-series comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the bank's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual banks or parts thereof.

Our goal is to make *Information Security for Banks: Operations, Technology, and Compliance* your go-to source implementing your security plans. If you have any suggestions regarding this manual, please let us know! You can e-mail me directly at diane.calmes@sheshunoff.com. You can also call our customer service representatives at 1-800-456-2340 if you have any questions regarding any of our products.

Sincerely,

Diane L. Calmes
Editor