Global Data Privacy and Security Team

FDIC Examinations At A Glance

FDIC bank examinations generally include a focus on the information technology ("IT") systems of banks with a particular focus on information security. The federal banking agencies issued implementing *Interagency Guidelines Establishing Information Security Standard*s (Interagency Guidelines) in 2001. In 2005, the FDIC developed the Information Technology—Risk Management Program (IT-RMP), based largely on the Interagency Guidelines, as a risk-based approach for conducting IT examinations at FDIC-supervised banks. The FDIC also uses work programs developed by the Federal Financial Institutions Examination Council (FFIEC) to conduct IT examinations of third party service providers ("TSPs").

The examination process relies to some extent on bank management attestations regarding the extent to which IT risks are being managed and controlled. Examiners focus their efforts on management-identified weaknesses and may confirm selected safeguards described by management as adequate. Nonetheless, reports by the Office of the Inspector General within the FDIC indicate that examiners may not be consistent in their review of the bank's compliance with the Interagency Guidelines and do not regularly provide a clear statement of adequacy on intrusion detection programs and incident response plans.

Number of IT examinations at financial institutions and technology service providers conducted by FDIC in a year.*	Time spent by FDIC to perform an IT examination at a financial institution found to have adequate security.*	Time spent by FDIC to perform an IT examination at a financial institution found to have some degree of supervisory concern.*	Percentage of Consent Orders issued in 2015 specifically citing deficiencies in IT as a basis for the Order. Over 50% involve either IT deficiencies or BSA and Compliance isues.
2,323	**8-10 DAYS**	**15-20 DAYS**	**20%**

*FDIC Office of Inspector General, Report No. EVAL-15-003 (Mar. 2015).

If you would like to be added to the distribution list for the Banking Group please visit the banking blog at blogs.bankrupt.com or to the data team go to bryancavedatamatters.com.

For more Information Contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
phone: 202 508 6000

Gerald L. Blanchard
Partner
gerald.blanchard@bryancave.com
One Atlantic Center, 14th Floor
1201 W. Peachtree St., N.W.
Atlanta, GA 30309-3471
phone: +1 404 572 6804

BRYAN CAVE

What bank directors should be thinking about when preparing for an examination:

- ✓ Is the Board comfortable that the Bank has management qualified to oversee all aspects of the Bank's IT operations, including compliance with all applicable IT laws and regulations?
- ✓ Is there a designated Vendor Management Coordinator in the Bank with an appropriate level of due diligence and vendor risk modeling experience for the type and quality of the Bank's IT services?
- ✓ Do the directors understand what IT services are being outsourced and whether the Bank's Vendor Management Program meets the requirements and guidance of the FFIEC IT Examination Handbook, *Outsourcing Technology Services*?
- ✓ Does the Bank's Business Continuity Planning/Disaster Recovery Plan ("BCP/DR" Plan) adequately address the sudden loss of IT services?
- ✓ When did senior management last review the organization's incident response portion of the Business Continuity Planning/Disaster Recovery Plan?
- ✓ Has the incident response plan been strategically tested (e.g., a breach tabletop simulation)?
- ✓ Has the incident response plan been operationally tested (e.g., a breach simulation)?
- ✓ Does the organization have a plan for how it would communicate a breach to bank customers, regulators and law enforcement?
- ✓ Has the organization retained cyber insurance coverage?
- ✓ Does management understand what is, and what is not, covered under the policy?
- ✓ Does the organization have external resources already identified, and under contract, to provide assistance in the event of a security incident?