Bank Directors Required to Face New (and Challenging) Information Technology Demands

By Thomas A. Brooks / Nov 23, 2015

In response to a Government Accountability Office report that found federal banking regulators were deficient in their ability to properly examine depository institutions' ability to protect against cyber risks, the FFIEC[1] recently amended its *IT Examination Handbook* that will vastly increase the obligations of a financial institution's Board of Directors to ensure that the institution is protected against cyber-attacks. As a result of the amendments, examiners are now directed to review almost 300 new specific items of inquiry during a bank's examination.

Examiners will focus on the new obligations imposed on the Board of Directors to oversee the management of the bank's cybersecurity program. As the new mantra has been phrased, "protection against cyber-attacks has been moved from the server room to the board room." Bank regulators have determined that their current highest priority in examining an institution is how to protect the institution and its depositors from cyber incursions - and that responsibility now rests firmly with the Board of Directors.

One of the examiner's objectives will be to determine whether the Board of Directors oversees, and senior management establishes, an effective governance structure that includes oversight of IT activities. To accomplish this, the examiner will review the institution's governance structure to determine the oversight of IT activities and *verify* that it includes the following:

- The Board sets the tone and direction for the bank's use of technology.
- IT risks are adequately identified, measured and mitigated.
- The Board has approved the information security program and other IT-related policies.
- The Board members are familiar with IT activities.

In order to verify that the Board is effective in its IT oversight, the examiner will specifically review and determine whether or not the Board does the following, among other things:

- Reviews and approves an IT strategic plan that aligns with the overall business strategy and includes an information security strategy to safeguard against ongoing and emerging threats, including cybersecurity threats.
- Oversees the institution's adoption of effective IT governance processes.
- Oversees management processes for approving third-party providers that include an assessment of financial condition and IT security posture of the third party, including cybersecurity.
- Has an oversight process that includes receiving updates on major projects, IT budgets, IT priorities, and overall IT performance; and has an approval process for critical projects and activities.
- Reviews the adequacy and allocation of IT resources in terms of funding and personnel.
- Approves a policy to escalate and report significant security incidents to the Board, steering committee, government agencies, and law enforcement, as appropriate.
- Holds management accountable for the identification, measurement, and mitigation of IT risks.

If the Board delegates certain activities regarding the oversight of IT to a committee, the examiner will determine whether the committee does the following:

- Maintains a charter that defines its responsibilities.
- Has a defined mission to assist the Board in IT oversight.
- Has decision-making authority.
- Receives appropriate management information from IT, lines of business, and external sources.
- Coordinates and monitors IT resources.
- Determines whether there is adequate training, including cybersecurity training, for institution staff.
- Reports to the Board on the status of IT activities to enable the Board to make decisions.
- Receives reports on IT to remain informed on risk.
- Is responsible for effective strategic IT planning, oversight of IT performance, and aligning IT with business needs.

The above descriptions provide a brief glimpse as to what the examiner will be doing to accomplish his/her objective of determining what a Board must do to properly oversee the IT activities of a financial institution. This is only one of 14 objectives that the examiner must accomplish in his/her examination. And, each objective requires the examiner to review several specific activities of the Board and management.

As mentioned at the outset, there are almost 300 specific elements that the examiner will review. Other specific areas of examination, to identify a few, include:

- A review of management's responsibility relating to business continuity should a cyber-breach occur.
- Determining the proper insurance coverage for cyber risk (including loss of hardware, software, litigation costs, damages from depositor suits, etc.).

- Enterprise risk management.
- Obtaining and retention of a qualified work force.
- Ensure that an institution is able to identify, control and mitigate risks.

Clark Hill PLC's Cybersecurity, Data Protection and Privacy team provides the legal expertise to work with financial institutions as they adjust to the requirements of the new cybersecurity era. Clark Hill's team approach to cybersecurity preparedness brings together attorneys from our core practice groups that are experienced in bank regulatory issues as well as information technology transactions.

For further information on the newly issued FFIEC Examination Procedures, contact Tommy Brooks at tbrooks@clarkhill.com | (202) 552-2356.

[1] The FFIEC comprises the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.