

## Risk-Focused Information Technology Examinations

By Maria Maestas

Senior Specialist, Risk and Compliance  
Compushare, Inc.

On December 4, 2007, the FDIC issued Financial Institution Letter FIL-105-2007 updating its Information Technology, risk-focused examination procedures. These enhanced procedures provide new insight into the areas of greatest regulatory concern for IT and information security, allowing each institution to create more comprehensive policies, procedures, and programs designed to protect these critical assets.

Some highlights of the update include:

- Enhanced Vendor Management oversight and Service Provider selection.
- Inclusion of new payment system risks such as credit card merchant processing, wire transfers, remote deposit capture, and ACH (automated clearing house).
- Increased focus on assessing risk (both IT assets as well as customer information) and the sufficiency of the controls.
- More comprehensive questions regarding compliance with Part 364, Appendix B, Interagency Guidelines Establishing Information Security Standards.

### Vendor Management/Service Provider Selection

The examination procedures now include more detailed questions specific to appropriate due diligence in the selection and ongoing maintenance of Vendors – especially Technology Service Providers. The level

of due diligence must be commensurate with the level of risk each vendor brings. Identifying inherent risk based on the vendor's financial impact to the institution or access to customer/consumer information is critical to establishing an appropriate program for ongoing reviews. All vendors should be reviewed and risk-rated with regards to their access rights and overall impact to the institution. This risk requirement is reiterated by the NCUA as part of their guidance letter 07-CU-13 issued in December 2007.

One way to accomplish this task is to create a spreadsheet with a list of all vendors; identify which are deemed critical based on their financial impact to the institution as well as their overall access to customer-sensitive information. Vendors with the most financial impact and access to the most information will have the greatest risk and thus require more in-depth due diligence. All vendors with access to or potential access to customer sensitive information (regardless of whether they transmit or store this information) should, at a minimum, require background checks of their employees, and provide proper insurance, bonding, and confidentiality clauses in their contracts.

### Payment System Risks

More attention is being focused on payment systems and ensuring that appropriate controls are in place to mitigate risks with regards to safeguarding customer information. Not all of these controls, however, are technical in nature. In accordance with the interagency guidelines, a comprehensive Information Security Program will include physical, technical and **administrative** controls which include oversight of the policies and procedures in both the operations department (dual controls, segregation of duties, customer due diligence, etc) and IT. Properly developed programs will include sound procedures that include ongoing training and testing in order to ensure these controls are effective at mitigating the associated risks.

It is highly recommended that all institutions

review their current policies to ensure the procedures are specific enough to provide adequate safeguards for protection of customer data. Many of the policies and procedures we review today are still too general to ensure proper oversight – reviewing exception/change reports on a “regular” or “as needed” basis will not provide adequate time to identify suspicious activity and take action before the information is potentially compromised. Procedures need to be more specific, but also realistic to ensure they will be followed. The best policies and procedures are deemed useless if they are not put into practice.

### Risk Assessment

Although frequently overlooked, a critical component of the Information Security Program is the development of a sound Incident Response Program. This was echoed in the FDIC's February 2008 Supervisory Insights:

*Even the best information security program may not identify every vulnerability and prevent every incident, so [Financial Institutions] are best served by incorporating formal incident response planning to complement strong prevention measures. In the event management's efforts do not prevent all security incidents (for whatever reason), Incident Response Programs (IRP's) are necessary to reduce the sustained damage to the [Institution].*

This guidance directs the institution to focus on the risk in its totality, recognizing that it is just as important to assess and evaluate both preventative and detective controls and their sufficiency in mitigating risk. This also validates the understanding that even the most comprehensive Information Security Program cannot “guarantee” the confidentiality, integrity and availability of customer information. We have to continue applying “layers” of security to help protect this vital asset.

The minimum requirements for an effective IRP require the inclusion of both reaction and notification procedures:



**Reaction Procedures for:**

1. Assessing security incidents that have occurred.
2. Identifying the customer information and information systems that have been accessed or misused.
3. Containing and controlling the security incident.

**Notification Procedures for:**

1. The institution's primary regulator.
2. Appropriate law enforcement agencies (and filing applicable SAR's).
3. Affected customers.

A properly developed IRP will also include ongoing training and testing to ensure the staff is capable of implementing the procedures as designed.

At least 32 states have passed laws requiring that individuals be notified of a breach in security resulting in the compromise or potential compromise of customer non-public information. This has subsequently increased regulatory attention devoted to incident response and has made the development of IRP's a legal necessity. A solid IRP will also be invaluable this year as institutions begin formulating strategic plans for combating identity theft.

**Information Security Program Self-Assessments**

The new FDIC examination procedures also include an outline for compliance with the Interagency Guidelines Establishing Information Security Standards. This outline can be an invaluable tool for use with self-assessments and ensuring a properly developed and executed Information Security Program.

The outline breaks out the requirements into manageable pieces and directly associates the requirement with the applicable item on the questionnaire. This helps with comprehension and understanding of the various mandates set forth by the applicable guidelines. These

mandates include:

1. Develop and implement a written Information Security Program.
2. Board of Directors involvement and oversight.
3. Perform a formal Risk Assessment at least annually.
4. Formalize a process to manage and control risk.
5. Oversee Service Provider Arrangements.
6. Adjust the Program based on results of third party reviews/audits, and analysis of risk.
7. Annual Report to the Board.

Whether this assessment be outsourced to a third party for assistance or performed in-house, having this "checklist" will help to ensure proper coverage for all requirements.

**Conclusion**

Safeguarding Customer Information has become a basic consideration for evaluating risk in all FFIEC IT programs. Whether the subject is business continuity, vendor management, payments, or even audits, identifying the critical information within that program has become a vital step for each. We are already seeing this new questionnaire being utilized by examiners; when it comes to safeguarding customer information, the harsh reality is that it's not a matter of "if", it's a matter of "when"... and we must all be prepared.