From the Examiner's Desk: Customer Information Risk Assessments: Moving Toward Enterprise-wide Assessments of Business Risk

Safeguarding sensitive customer information is both a statutory responsibility and a business imperative for financial institutions. Despite the fact that financial institutions have been required to implement information security programs since mid 2001, the results of information technology (IT) examinations often indicate that institutions struggle with conducting effective risk assessments. In addition, guidance and industry best practices for assessing information security risks continue to evolve, resulting in a variety of approaches to this important business function.

Effective risk assessments are even more important today than they were in 2001. Financial institutions are the target of increasingly sophisticated cyber attacks perpetrated by well-funded criminal enterprises around the world. These cyber attacks target sensitive customer information, as well as other information assets and electronic payment channels, to commit the 21st century equivalent of old-fashioned bank robbery. Stolen customer information is used to make fraudulent credit and debit card purchases, and stolen customer identity credentials are used to compromise electronic payment systems and siphon funds from customer accounts.

This article summarizes three types of risk assessments, identifies issues and areas for improvement often observed by examiners, and discusses the supervisory response to deficiencies.

Background

Section 501(b) of the Gramm-Leach-Bliley Act establishes a requirement for financial institutions to safeguard the privacy of customer financial information.[1] The banking agencies provided guidance on meeting these requirements in *Interagency Guidelines Establishing Information Security Standards* (*Information Security Standards*).[2] The *Information Security Standards* require financial institutions to assess risk to customer information or customer information systems. FDIC examiners (when conducting an IT examination and assigning an IT rating) must assess the quality of an institution's risk assessment methodologies as part of the examination.[3]

The nature, type, and depth of risk assessments are affected to varying degrees by regulatory requirements, supervisory processes, and industry best practices. As financial institution operating environments, product and service offerings, and outsourcing arrangements differ, risk assessment guidance has taken the approach of setting forth general principles. This flexible approach is needed to accommodate the unique characteristics and risk profiles of financial institutions; however, as a result, the nature and quality of risk assessments vary. Nonetheless, risk assessment approaches typically fall into three categories:

- ***Customer information risk assessments***, which seek to comply with

[1] See 15 U.S.C. 6801 and 6805(b) of the Gramm-Leach-Bliley Act and Appendix B to Part 364 of the FDIC Rules and Regulations, http://www.fdic.gov/regulations/laws/rules/2000-8660.html#fdic2000appendixbtopart364.

[2] See FIL-22-2001,"Security Standards for Customer Information," March 14, 2001, http://www.fdic.gov/news/news/financial/2001/fil0122.html.

[3] For further information, see FIL-81-2005, "Information Technology Risk Management Program (IT-RMP) New Information Technology Examination Procedures," August 18, 2005, http://www.fdic.gov/news/news/financial/2005/fil8105.html; and FFIEC IT Examination Handbook, Information Security Booklet, July 2006, http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#infosec.

the requirements of the *Information Security Standards* by focusing on risks to customer information or customer information systems.

- ***Information security risk assessments***, which expand on customer information risk assessments by assessing risks to all information assets, as recommended in the FFIEC *Information Security Booklet*.[4]
- ***Enterprise-wide assessments of business risk***, which assess risks across all business lines, including, but not limited to, risks to information security.

Examiners may encounter any of these types of risk assessments and, therefore, should understand their differences and limitations. The next section describes these risk assessment approaches and highlights observations from IT examinations and the supervisory response to deficiencies.

Customer Information Risk Assessments

Customer information risk assessments often represent a "compliance response"—the actions a financial institution takes to meet the requirements of the *Information Security Standards*. To the extent these risk assessments reflect an attempt to comply with minimum standards, they may not fully address the intent of the standards. As a result, they may fall short of identifying and mitigating threats to customer information or customer information systems.

Consistent with the *Information Security Standards*, customer information risk assessments typically are intended to accomplish the following:

1. Identify customer information or customer information systems.
2. Determine reasonably foreseeable internal and external threats to customer information or customer information systems (e.g., threats that may affect the confidentiality, integrity, or availability of customer information in paper-based and electronic form).
3. Determine the likelihood and potential damage of these threats, in terms of cost, time, or reputation, through a quantitative or qualitative analysis.
4. Assess existing policies, procedures, customer information systems, and other arrangements to control risks.

The *Information Security Standards* require banks to address the risks identified by their customer information risk assessment by the use of appropriate controls that should be included in the bank's information security program. A pre-requisite for such risk-mitigating action is an effective risk assessment. IT examinations, however, often determine that customer information risk assessments fall short in one or more respects. These are discussed below.

Relevant Internal and External Vulnerabilities

Relevant internal and external vulnerabilities, particularly those involving unauthorized or inappropriate employee actions,[5] often go unrecognized during the customer information risk assessment process. Examples include insufficient separation of duties, excessive user access rights, and inappropriate review of audit logs and account maintenance reports. In addition, vulnerabilities originating from outsourcing or service provider arrangements—another form of trusted

[4] See FFIEC IT Examination Handbook, *Information Security Booklet*, July 2006, http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#infosec.

[5] These often represent the foundation for fraud or for misappropriation of funds.

continued from pg. 25

third-party relationship—may not be identified as part of a customer information risk assessment. These vulnerabilities include improper encryption of electronic information in transit or in storage at the third-party location, insufficient background checks on third-party employees with access to nonpublic customer information, and insufficient oversight of third parties' subsequent subcontracting of services to entities unknown to the financial institution, including entities that may operate outside the United States.[6] Also, risk assessments looking for external vulnerabilities should identify the threat posed by cyber criminals using phishing scams and malicious software to compromise customer accounts and fraudulently transfer funds, thereby posing reputation and financial risk to the institution.

Inherent and Residual Risks

Customer information risk assessments may assume that controls are functioning as intended and thus may convey results that could give senior management and the Board of Directors a false sense of security. A key to avoiding unpleasant surprises in this regard is to clearly differentiate between, and adequately assess, inherent and residual risks. Inherent risks are the risks that exist before the application of controls intended to mitigate those risks. Clearly identifying inherent risks is particularly beneficial in making determinations for the scope and frequency of audit and independent reviews—determinations that should be based on a financial institution's assessment of inherent risk without assuming that controls are functioning as intended. Residual risks are those that exist after the application of controls. In this context, risks cannot be completely eliminated, even though layered security may reduce risk to an acceptable level. To evaluate the extent of residual risk, financial institutions should consider the effectiveness of their administrative controls, such as policies, procedures, and employee training; physical controls, such as locking doors, cabinets, and alarms; and logical controls, such as passwords, encryption, virus protection, and firewalls.

Emerging Risks

As the *Information Security Standards* require financial institutions to periodically evaluate and modify information security programs, management also should ensure that a key component of the program—the risk assessment methodology—is revisited before changes in business lines, service offerings, or outsourcing arrangements occur. Unfortunately, when the risk assessment process is approached as a compliance response to the standards, it may not adequately assess emerging risks. However, when a risk assessment is approached as a value-added process, the resulting document can effectively support key business decisions. A financial institution can reasonably determine whether proposed changes in business lines, service offerings, or outsourcing arrangements can be accomplished within approved risk tolerances, and, if not, what actions should be taken to ensure they are.

Result Reviews

As a financial institution's risk profile evolves, so should its risk assessment results. An opportune time to revisit risk assessment results is when controls are subject to periodic audit or independent review. These reviews should provide evidence that the controls are achieving their intended purpose (i.e., reducing risk as indicated by the risk assessment). In turn, a financial institution is afforded the opportunity to validate the basis for its final risk determinations. For

[6] See FIL-52-2006, "Foreign-Based Third-Party Service Providers: Guidance on Managing Risks in These Outsourcing Relationships," June 21, 2006, http://www.fdic.gov/news/news/financial/2006/fil06052.html.

example, a risk assessment may indicate that controls surrounding the institution's ability to recover from a disaster event are effective and result in a low level of residual risk, while an audit of disaster recovery/business continuity strategies indicates that plans are out-of-date and untested. In this example, the financial institution should revisit residual risk determinations and may need to develop a mitigation strategy to improve the risk profile. Audit/independent reviews also may aid the risk assessment process by identifying other information assets that require protection—a need management may not have previously considered.

Mitigation Plans and Supervisory Corrective Action

Assuming that an element of risk exists after the application of controls, management must determine whether it will accept, transfer (i.e., insure), or further address residual risk by developing mitigation plans for unacceptable risks. The Prouty Approach[7] is one example of a way to make these determinations based on the loss severity (impact) and the loss frequency (likelihood) of a risk event (see Table 1).

We reproduce this matrix not as an endorsement of this or any specific formulaic approach to risk mitigation, but as a reminder that the customer information risk assessment should not end with the assessment, but should result in concrete steps to correct material deficiencies. Often, customer information risk assessments remain silent about further actions that may be needed to mitigate residual risk. As a result, the value of the assessment as an effective management tool may be limited.

From a supervisory perspective, the requirement for banks to safeguard customer information is statutory and not subject to management discretion. Therefore, when the bank's information security risk assessment, the results of its internal reviews or audits, or the examiner's own analysis finds that customer information is not adequately safeguarded, corrective action should be required.

According to outstanding IT examination procedures, examiners should address material departures from guidance in the *Information Security Standards*. A financial institution may be subject to criticism in the Risk Management Report of Examination and potentially cited for a contravention of interagency guidance on the Violations of Laws and Regulations page.[8] Further, as delineated in the Uniform Rating System for Information Technology,[9] insufficient risk assessment processes may impact a financial institution's assigned IT rating. In egregious instances, a financial institution also may be exposed to Civil Money

Table 1

The Prouty Approach

		Loss Frequency			
		Almost Nil	**Slight**	**Moderate**	**Definite**
Loss Severity	**Severe**	Transfer	Reduce/prevent	Reduce/prevent	Avoid
	Significant	Retain	Transfer	Reduce/prevent	Avoid
	Slight	Retain	Transfer	Prevent	Prevent

[7] Timothy Abram, "The Hidden Values of IT Risk Management," *ISACA Journal*, volume 2, 2009, pg. 4.

[8] Absence of an information security program, a seriously deficient program, or significant noncompliance with the *Information Security Standards* should be addressed on the Violations of Laws and Regulations page.

[9] See FIL-12-1999, "Uniform Rating System for Information Technology," February 5, 1999, http://www.fdic.gov/news/news/financial/1999/fil9912.html.

continued from pg. 27

Penalties, depending on the degree of noncompliance or management's disregard for securing customer information. However, in less significant instances where a risk assessment only focuses on customer information or customer information systems, examiners should encourage financial institutions to expand risk assessment methodologies beyond customer information to include other information assets, consistent with outstanding guidance.

Information Security Risk Assessments

As noted above, customer information risk assessments often are developed to comply with a specific statutory requirement to safeguard customer information. As such, they often do not include an assessment of risk to other information assets. Examples of such assets, which may be subject to the same threats and vulnerabilities as customer information assets, include, but are not limited to, the following:

- Trade secrets
- Strategic plans and objectives
- Human resource records
- Authentication credentials
- Network topologies/schematics
- Source code libraries
- Proprietary software
- Executive Committee/Board minutes

The disclosure, alteration, or destruction of such information may materially affect the success and viability of the financial institution. As a result, these assets deserve management's consideration under a risk assessment framework.

Information security risk assessments evaluate risk to all information assets, as suggested in the FFIEC *Information Security Booklet*. Security weaknesses are not limited to customer information and customer information systems and can increase exposures in other operational areas. Further, security concerns in these areas can quickly erode customer confidence and adversely affect the viability of strategically important products and services. For example, a security incident resulting from compromised corporate cash management authentication credentials could affect a financial institution's ability to attract and retain corporate accounts and related lending relationships. As such, financial institutions should ensure that information security risk assessments adequately consider potential risk in all business lines and risk categories.

Customer information risk assessments and information security risk assessments have similar expectations and limits. Both approaches must identify information assets, determine threats and vulnerabilities, evaluate impacts, and assess controls. Also, information security risk assessments must address many of the same types of issues as customer information risk assessments, including the following:

- Consideration of relevant internal and external vulnerabilities
- Delineation of inherent and residual risks
- Assessment of emerging risks
- Revisiting risk assessment results
- Development of mitigation plans

Given similar expectations and limitations of customer information and information security risk assessments, examination reviews will be similar—with one notable exception. When reviewing an information security risk assessment, examiners also should consider the extent to which management reasonably identifies and classifies information assets. Under a customer information risk assessment, data classification is of less importance, as all information is confidential customer information. However, as an information security risk

assessment expands beyond customer information to include information of varying importance and sensitivity, management should incorporate data classifications (e.g., public, private, sensitive, or confidential) into its methodology. Such effort is necessary to help direct management attention to the information assets that are most sensitive or critical to the business process and thus most deserving of scarce financial and staff resources.

Consistent with the approach taken for customer information risk assessments, examiners should address material departures from guidance in the *Information Security Standards* and implement a similar supervisory response based on the nature of the findings and effectiveness of the risk assessment methodology. Although these deficiencies may not constitute a violation of law or regulation, they can be subject to specific criticism in the Report of Examination and may impact a financial institution's IT rating. Examiners also should encourage financial institutions to ensure that information security risk assessments convey findings in terms of their impact on business risk.

Enterprise-Wide Assessments of Business Risk

Recent efforts to meld enterprise risk management with information security risk management represent a significant opportunity for financial institutions to gain material benefits and economies from their risk assessment methodologies. Such assessments typically incorporate the following:

- Assessing enterprise-wide risks to the business (not only those relating to information security) and how the use of technology relates to those risks;
- Identifying how data are used for critical business processes (sometimes referred to as mapping business processes); and
- Evaluating risk assessment results in terms of their impact on business risk.

This approach helps achieve enterprise-wide goals and objectives and assists senior management and the Board of Directors in understanding and managing risks. Although guidance on this approach remains formative, key steps include:

1. *Identifying enterprise risks* that may affect the institution (typically performed by senior management or the Board of Directors who own the risk).
2. *Defining business processes* that drive enterprise risks.
3. *Assessing business process risks*.
4. *Linking technology to the business processes* (e.g., identifying threats, vulnerabilities, impacts, and controls) and focusing efforts on higher risks that support the business process.
5. *Developing plans and strategies* to further manage business risks and mitigate risks that are outside approved tolerances.

As this process differs from those of a typical customer information risk assessment or information security risk assessment (which usually are structured around the applications or systems that store such information), an enterprise-wide assessment of business risk is best illustrated by an example.

1. *Identifying enterprise risks*—The Board of Directors identifies internal abuse/fraud as an enterprise-wide risk.
2. *Defining business processes*—Management identifies the lending business process as a key driver of the risk of internal abuse/fraud.
3. *Assessing business process risks*—Management identifies the risk of improper boarding of loans and altering payment and past-due status

continued from pg. 29

as critical fraud risks within this business line.

4. *Linking technology to the business process*—Based on the risks selected, management evaluates threats and vulnerabilities within the loan application and makes inherent and residual risk determinations after an analysis of controls, which in this case may include access controls, user rights, oversight/independent review processes, and interconnectivity with network and peripheral devices.

5. *Developing plans and strategies*—By completing this assessment and reviewing other enterprise risks, management can focus on higher risks evident in key business processes and adjust the scope of audit/independent review programs accordingly. For example, instead of reviewing access controls and user permissions as part of loan, deposit, and IT general control audits, the Board may prescribe an overall review of logical access controls that focuses on functions most relevant to key business process risks.

Examiners are reminded that existing guidance does not require enterprise-wide assessments of business risk. However, the FFIEC *Information Security Booklet* indicates that financial institutions should ensure that information security risk assessments adequately consider potential risk in all business lines and risk categories. Given the absence of specific guidance, examiners must use judgment in evaluating how enterprise-wide assessments of business risk are used. Examiners also should consider customer information and information security guidance in the *Information Security Standards* and the FFIEC *Information Security Booklet*.

Conclusions

Although customer information risk assessments, information security risk assessments, and enterprise-wide assessments of business risk differ, consideration of their inherent characteristics and limitations creates an opportunity to enhance the effectiveness and usefulness of all three models. In all instances, financial institutions must comply with the requirements of the *Information Security Standards*. Bankers and examiners also need to be cognizant of the potential shortcomings of the more limited forms of risk assessments, such as insufficient internal and external threat identification, improper delineation between inherent and residual risk, untimely assessment of emerging risk, improper revisiting of risk assessment results, and failure to develop risk mitigation strategies as needed. Lastly, to improve the scope of assessments and comply with FFIEC guidance, risk assessments should include all information for which a security breach could materially affect an institution's risk profile. Ideally, risk assessment findings should be tied to business risks more broadly. These efforts will help ensure that senior management, the Board of Directors, and the institution's regulators gain sufficient insight into the institution's true risk posture and help reduce the potential for an unforeseen, escalated risk profile. In view of the sophisticated cyber threats to information assets, effective risk assessments are the foundation on which financial institutions should build a comprehensive and effective risk mitigation program.

Paul M. Onischuk
Examination Specialist (IT)
Division of Supervision and Consumer Protection
Chicago Regional Office
ponischuk@fdic.gov