From the Examiner's Desk: The Evolution of Bank Information Technology Examinations

This regular feature focuses on developments that affect the bank examination function. We welcome ideas for future columns, and readers can e-mail suggestions to ***SupervisoryJournal@fdic.gov****.*

The Federal Deposit Insurance Corporation (FDIC) has conducted information technology (IT) examinations for more than forty years.[1] In recent years, the review of financial institutions' information security programs has taken on increased importance because of the growing incidence of denial-of-service attacks, account takeover fraud, foreign espionage, hackers, and complex technology partnerships. The escalating nature of cyber threats targeted at financial institutions and their customers makes IT security and operational controls critical to the safety and soundness of the institution. This article discusses the evolution of IT examinations of financial institutions and technology service providers (TSPs), with a focus on the current examination program goals, processes, and effective approaches to IT risk management.

Background

As part of the examination process, the FDIC and other financial regulatory agencies review and assess financial institution records. Decades ago, as financial institutions began to use computerized accounting systems, concerns increased about access to those records and the accuracy of the systems processing them.

Initially, computing systems were only available to the largest financial institutions due to their high cost. However, in 1962, the Bank Service Company Act[2] (BSCA) was enacted to enable financial institutions to invest in bank service companies, with prior regulatory approval. Bank service companies provided a vehicle for one or more smaller financial institutions to invest in an entity to provide those institutions with IT services. As a result, the use of computerized accounting systems expanded among smaller financial institutions. The BSCA also permitted institutions to contract with independent service providers, with prior notice to their primary federal regulator.

The FDIC formalized the EDP examination requirement in 1970, following a similar trend by the audit industry. All FDIC field offices selected certain examiners to complete a training course in EDP examinations. Early examinations focused on the integrity of electronic data systems, internal controls, and physical security. There was recognition at the time that reliance upon computers increased the potential for computer-based fraud or embezzlement. Major TSPs were examined to ensure the servicer did not disclose confidential financial institution data and the outsourcing of EDP was not an attempt to hide evidence of fraud or other unsafe-and-unsound conditions in the institution. The goal, whether for in-house or outsourced data processing examinations, was to ensure the data processing function could reliably provide accurate processing of transactions and records. Although these early examinations

[1] These examinations were formerly referred to as electronic data processing (EDP) and then information systems (IS).

[2] Public Law No. 87-856, 12 U.S.C. 1861 et seq. See http://ithandbook.ffiec.gov/media/27536/con-12usc1861_1867c_bank_service_company_act.pdf.

were able to identify issues with controls and other management practices that could affect the safety and soundness of these automated records, this process did not have defined standards for measuring risk.

Regulatory authority over TSPs was greatly expanded as a result of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRIRCA).[3] FIRIRCA created the Federal Financial Institutions Examination Council (FFIEC). The FFIEC established standards for EDP operations by developing the EDP Examination Handbook,[4] creating an EDP examination rating system and establishing a formal program for the joint examination of service providers. The new rating system applied to bank-owned data centers and nonbank service providers. The EDP rating criteria of 1978, which addressed audit, management, systems development and programming, and computer operations, were maintained until 1999. At that time, the rating system was revised to the new Uniform Rating System for IT (URSIT), which included replacing two components[5] and revising the numerical rating definitions to conform to the rating definitions of the Uniform Financial Institutions Ratings System, commonly referred to as the CAMELS rating system.

Through an amendment to the BSCA,[6] FIRIRCA gave the FDIC and other financial institution regulators authority to examine service providers and changed the approval requirement to allow for after-the-fact notice of service provider arrangements. Prior to FIRIRCA, financial institutions were required to provide notice to, and receive permission from, their regulator before contracting with a service provider. Regulatory approvals were based, in part, on contractual agreements that permitted regulatory access to the institutions' records at the service provider. Table 1 lists other milestones in the evolution of the IT examination.

Table 1: IT Examination Milestones

Date	Milestone
1962	Bank Service Company Act allows small financial institutions to compete with large institution technology through investments in joint bank service companies.
1970	FDIC begins examinations of financial institution computer operations.
1977	First edition of Control Objectives published by Electronic Data Processing Auditing Association (EDPAA).
1978	Interagency EDP Examination, Scheduling, & Report Distribution Policy Statement published. FDIC authorizes 24 EDP examiner slots. Interagency Uniform Rating System for Data Processing Operations introduced.
1980	FFIEC EDP Examination Handbook published.
1982	Multi-Regional Data Processing Servicer Program (MDPS) founded.
1999	Uniform Rating System for Information Technology revised to conform with Uniform Financial Institution Rating System.
2002	FDIC combines e-banking, serviced bank, information security, and EDP work programs, and requires IT examinations and IT ratings of all FDIC-supervised financial institutions.
2005	FDIC issues IT Risk Management Program (IT-RMP) to implement a risk-focused approach to IT examinations and follow the requirements of the Interagency Guidelines Establishing Information Security Standards. IT-RMP was revised in 2007.
2010	FDIC requires all risk management examiners to take the IT Examination Course within 6 months of the commissioning process, as well as 3 other basic IT courses, to better prepare them for evaluating IT risks in financial institutions.

[3] Section 308 of Public Law No. 95-630.

[4] The EDP Examination Handbook has been extensively revised over the years and is published as the FFIEC IT Handbook at http://ithandbook.ffiec.gov/it-booklets.aspx.

[5] The last two components were replaced with "Development & Acquisition" and "Support & Delivery."

[6] See footnote 3.

continued from pg. 21

Banking Risks Today

Although fraud and availability of records remain critical safety-and-soundness concerns, financial institutions and regulators must address a growing array of cyber threats to institutions and their customers. Cyber criminals are continuing to develop new means of accessing personal and institutional accounts, political activists seek attention by disrupting banking services, and foreign powers try to access corporate networks to steal proprietary business information. Vulnerability to these attacks can heighten an institution's reputational risk and diminish confidence in the overall banking system. These attacks also can affect a financial institution's liquidity and capital positions, as discussed later in this article. Bankers increasingly are asking their regulators for guidance on how to address this constant-threat environment. However, requiring institutions to develop and implement specific technical controls often lags the threat and redirects management from the development and maintenance of a robust and effective security program to focusing strictly on regulatory compliance. Bankers should understand that a security program encompasses more than technology. A security program addresses how the business operates in today's overall risk environment.

Today's IT Examination Goals

Today, most financial institutions rely on IT systems, external service providers, and Internet-connected applications to provide or enable key banking functions. IT is part of the infrastructure for all business units. Therefore, IT governance should be viewed as an important part of corporate governance more generally, and financial institutions should consider industry standards for IT governance.[7] The FDIC's IT examination philosophy has placed increasing emphasis on institutions' practices and procedures for managing IT risks, including third-party risk, protection of sensitive customer information, and reputation risk. In 2002, the FDIC combined the examination programs for IT, e-banking, serviced banks, and Gramm-Leach-Bliley Act[8] (GLBA) compliance into a single function. The combined IT examination was migrated to the safety and soundness Report of Examination to engage executive management on issues related to technology risk management. This combination emphasized that IT and operational risks can affect an institution's safety and soundness.

The FDIC examines a financial institution's IT operations because they support the overall enterprise. IT operations must protect the institution's financial health. Financial institutions ultimately fail because of inadequate liquidity or capital, not because of a broken computer. However, electronic operations can have a direct and sometimes immediate impact on liquidity or capital. Computer failures that prevent or delay the presentment and settlement of transaction items can directly affect an institution's liquidity. The longer a financial institution's systems are unable to present items to settle with correspondent banks, the higher the probability the institution may need to borrow funds or sell assets to cover account shortages. New types of cyber fraud, such as commercial account takeover fraud, may result in

[7] See COBIT: Framework for IT Governance and Control at http://www.isaca.org/resources/cobit.

[8] Public Law No. 106-102. See http://www.fdic.gov/regulations/laws/rules/2000-8660.html#fdic2000appendixbtopart364.

losses that can exceed the required capital of the financial institution.

Third-party risk appears to be one of the most significant IT-related risks. This is due to the fact that externally controlled services and products, such as credit and payment products offered in conjunction with third-party non-financial providers, have been integrated into a financial institution's products and services.[9] Risk tolerance levels can easily be exceeded without an adequate level of control or expertise in these products. Even though technology makes integration easy, oversight requires a technical and a business perspective.

The regulatory emphasis on protecting customers' sensitive digital information became most apparent with the promulgation of the GLBA information security guidelines in 2001.[10] These guidelines require financial institutions to implement a comprehensive information security program to ensure the safety and confidentiality of customer information. Although these guidelines were based on established computer security principles, they expanded the regulatory focus beyond protecting the institution's information to protecting the customer's information. These guidelines do not require specific technical controls. Instead, they require the development and implementation of a broad risk management program that addresses risk identification and assessment, implementation of policies and procedures to mitigate risks, employee training, reporting, and the involvement and approval of the board of directors. Because of these new guidelines, the FDIC examination process refocused on these risk management principles. This shift was challenging for financial institutions and examiners as it relied less on prescriptive technical controls and more on governance and oversight.

In addition, reputational risk is a more difficult thing for examiners to assess. Frequent system failures, electronic account fraud, and other cyber incidents can weaken the public's confidence in a financial institution or the overall banking system. In 2005 and again in 2011, the federal banking agencies raised the level of expectations for online banking by requiring stronger authentication of customers logging into online banking systems.[11] Examiners now evaluate and assess if an institution is in conformance with supervisory guidance relating to the reliable authentication of customers using online banking systems.

Today's IT Examination Process

Today, the FDIC conducts examinations of a financial institution's risk management practices related to ensuring adequate controls for the confidentiality, integrity, and availability of sensitive and critical records, in both electronic and paper form.

[9] See "Mobile Payments: An Evolving Landscape," ***Supervisory Insights***, Winter 2012 at www.fdic.gov/regulations/examinations/supervisory/insights; "Payment Processor Relationships: Revised Guidance," FIL-3-2012, January 31, 2012 at http://www.fdic.gov/news/news/financial/2012/fil12003.html; "Third Party Risk: Guidance for Managing Third Party Risk," FIL-44-2008, June 6, 2008 at http://www.fdic.gov/news/news/financial/2008/fil08044.html; "Foreign-Based Third-Party Service Providers: Guidance in Managing Risks in These Outsourcing Relationships," FIL-52-2006, June 21, 2006 at https://www.fdic.gov/news/inactive-financial-institution-letters/2006/fil06052.html.

[10] 12 CFR 364, Appendix B.

[11] See "Federal Financial Institutions Examination Council Guidance on Authentication in an Internet Banking Environment," FIL-103-2005, October 12, 2005 at https://www.fdic.gov/news/inactive-financial-institution-letters/2005/fil10305.html; "Federal Financial Institutions Examination Council Supplement to Authentication in an Internet Banking Environment," FIL-50-2011, June 29, 2011 at https://www.fdic.gov/news/inactive-financial-institution-letters/2011/fil11050.html.

Bank Information Technology Examinations

continued from pg. 23

IT examinations are conducted by examiners with specialized training in technology risk management. IT examination programs fall into two categories: financial institution examinations and TSP examinations.

The federal banking agencies have published supervisory guidance and examination work programs as part of the FFIEC IT Examination Handbook.[12] The guidance in the Handbook applies to financial institutions and TSPs. The Handbook consists of eleven booklets covering audit, business continuity planning, development and acquisition, e-banking, information security, management, operations, outsourcing technology service providers, retail payment systems, wholesale payment systems, and supervision of technology service providers. These booklets focus on an institution's or TSP's use of effective risk management practices, such as risk assessments, business impact assessments, independent audits, and vendor management.

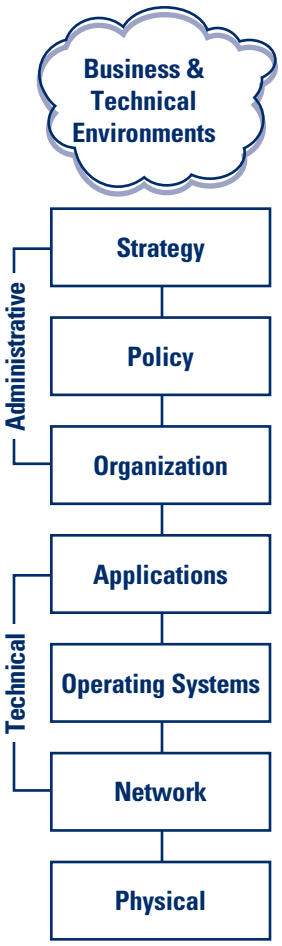
IT examinations are not "one size fits all." When determining the scope of an examination, particularly for community financial institutions, examiners will consider the size and complexity of the institution's IT operations. The FDIC's IT-RMP provides a range of examination levels. IT-RMP does not attempt to examine every institution with the full set of FFIEC IT Examination Handbook work programs. Such an effort would be overwhelming for the examiner and the institution. Instead, the examination scope is based on the complexity of the IT infrastructure, as determined by the results of the Technology Profile Script (TPS) and the financial institution's responses to the IT Officer's Questionnaire, combined with other factors that examiners consider, such as issues identified in the prior examination or cyber incidents that may have occurred since the last examination. Examiners complete the TPS, which yields an overall score reflecting the complexity of the institution's IT infrastructure. The IT Officer's Questionnaire asks a series of questions concerning the financial institution's risk management processes, which the institution answers and returns to the FDIC. These activities help the examiner determine the depth and focus of the examination.

Effective Approaches to IT Risk Management

In addition to assessing and managing risk, the GLBA information security standards provide guidelines on administrative, technical, and physical controls. These may be viewed as the basis for a layered approach to information security and can effectively link enterprise governance and technology governance. Today's Chief Executive Officer should understand how technology and supporting processes enable a financial institution to achieve its business goals. A business decision to enter a new market or offer a new product may hinge on what technology products are available (or need to be created) to achieve that goal. The following are five strategies financial institutions should consider in managing their use of information technologies.

[12] Federal Financial Institutions Examination Council: FFIEC Examination Handbook InfoBase at http://ithandbook.ffiec.gov/it-booklets.aspx.

- Think strategically. Today, it is impossible for financial institutions to implement a new product or service without technology. An institution's information security program should be integrated with its strategic goals and objectives. Security should meet the business need, and vice versa, and should be considered when establishing business cases, budgets, IT project planning, staffing, and policies. Significant events such as changes in partners, systems, or market segments may warrant a strategic review of information security.
- Guide a bank with policies. A financial institution's security strategy and technology should drive the types of policies put in place. Security policies can be written for a variety of technical or administrative subjects. Examples include acceptable-use policies, business continuity policies, information disposal policies, and server configuration policies.
- Control the organization. Organizational controls deal with people and may be thought of as the "human firewall." Whether a financial institution is establishing an information security office at the appropriate level, segregating duties or functions that could result in fraud, training staff about security risks, or conducting background checks, people are the key interface between policies and technology.
- Control the technology. Technical controls generally involve hardware, software, and networks. Finding the best technical control is a balance between security and functionality, and a critical defense against cyber threats. Perimeter security, access



control, configuration management, and intrusion detection are constantly changing. Regulators generally do not require specific technical controls as these could become outdated before they are published. Effective risk assessment should be the guide. Today, information sharing is key to the development and implementation of the most current and effective technical risk controls. Organizations such as the United States Computer Emergency Response Team (US CERT),[13] the Financial Services Information Sharing and Analysis Center

[13] US CERT is the operational arm of the Department of Homeland Security's National Cyber Security Division and leads efforts to improve the nation's cyber security posture.

continued from pg. 25

(FS-ISAC),[14] and trade associations share information about the latest threats and potential fixes to those threats.

- Don't forget the physical. Physical controls are concerned with the protection of facilities and infrastructure from environmental, human, and systemic threats. These include limiting access to critical or sensitive systems, maintaining adequate inventory, properly disposing of used equipment, and ensuring facilities are resilient from physical threats.

The Future of IT Examinations

Technological innovation allows financial institutions to change the way they do business. However, effective risk management practices often lag these innovations. The FDIC continues to review and evaluate emerging technologies to determine the potential impact on an institution's IT operations.

Moreover, cyber threats are growing, with many threats coming from outside our borders. The future cyber security model for banking must address the bigger picture of how each financial institution maintains stability and security from these new threats. On February 12, 2013, President Obama issued an Executive Order entitled *Improving Critical Infrastructure Cybersecurity*[15] and Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience.*[16] These orders require that a cybersecurity framework be developed for each critical infrastructure sector of the U.S. economy, including financial services, water and wastewater systems, communications, energy, and public health.

The framework developed by the federal bank regulators is an ongoing process and will continue to be evaluated and strengthened over time. In keeping with the spirit of the Executive Order, the FDIC will participate in the development of this new framework in cooperation with the National Institute for Standards and Technology. Through these and other ongoing efforts, the FDIC remains committed to ensuring that IT security standards for financial institutions promote safety and soundness, protect consumers, and continue to allow for business innovation.

Jeffrey Kopchik
Senior Policy Analyst
Division of Risk Management Supervision
jkopchik@fdic.gov

Donald Saxinger
Senior IT Examination Specialist
Division of Risk Management Supervision
dsaxinger@fdic.gov

[14] FS-ISAC was established by the financial services sector in response to Presidential Directive 63 which mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to protect U.S. critical infrastructure.

[15] The White House, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[16] The White House, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.